T.I.S.P. Community Meeting 2010

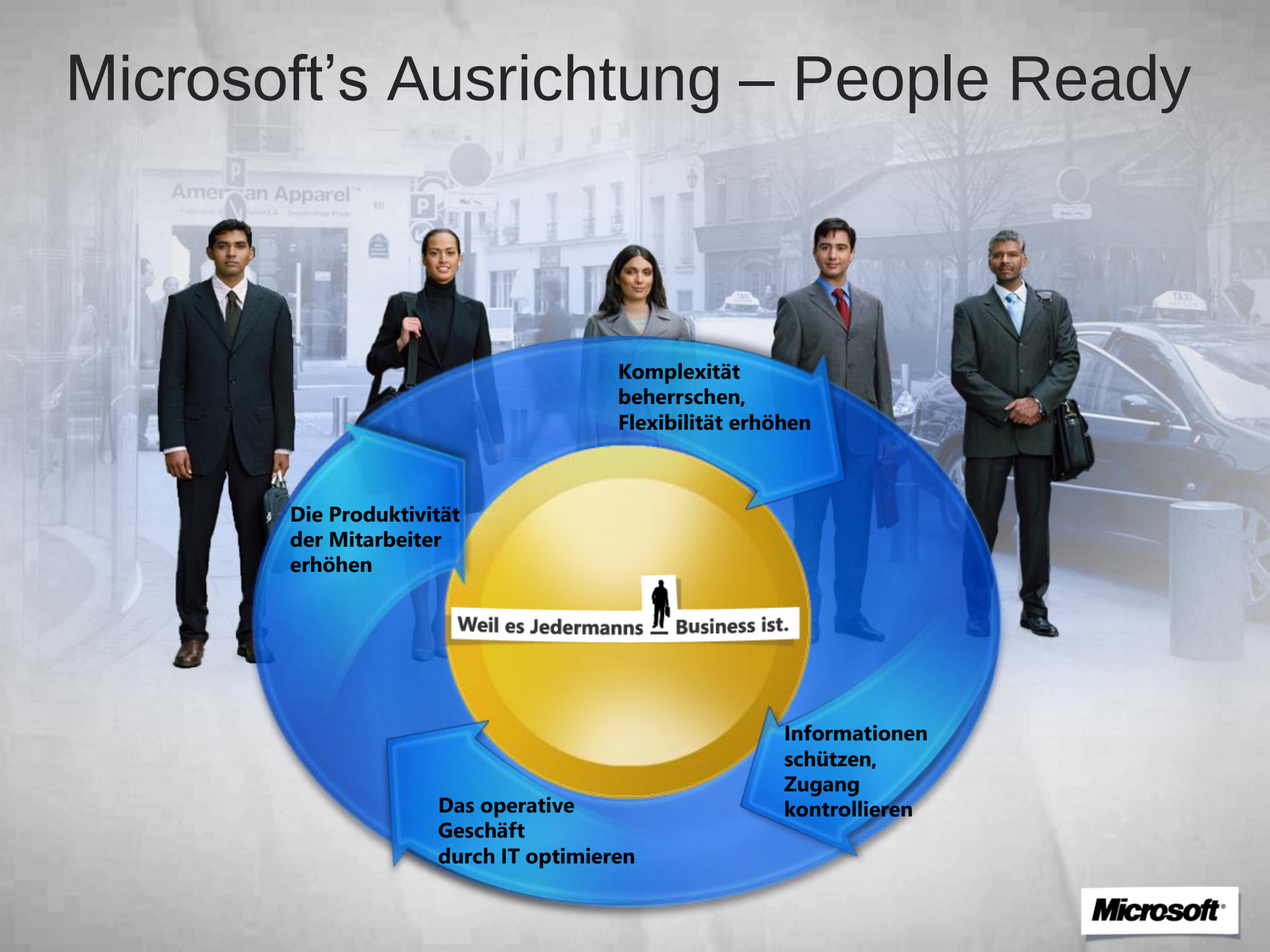
Köln, 03./04.11.2010

Michael Kranawetter
Chief Security Advisor
Michael.Kranawetter@microsoft.com

Microsoft Deutschland GmbH Unterschleißheim

Sicherheitsaspekte

Microsoft’s Ausrichtung – People Ready



Microsoft

Die Anforderungen der Geschäftsseite

User Experience

- IT-Zugriff überall und jederzeit
- Vielfalt an Devices
- Benutzerfreundliche Oberflachen

Serviceorientierung

- Service Level Agreements (SLA)
- Geschäftliche Funktionalitäten
- User-centric Service Level Metrics

Nutzenabhängige Kosten

- Abrechnung nach Verbrauch
- Flexible Bezahl-/ Geschäftsmodelle
- Pay as you grow

Microsoft

Und die Herausforderungen auf IT Seite

IT Kosten senken

- Serverkonsolidierung und Sizing
- Energie- und Platzverbrauch reduzieren
- Kompatibilität der Anwendungen

IT Effizienz erhöhen

- Schnelle Beschaffung & Deployment
- Hohe Verfügbarkeit, Saklierung
- Sicherheit und Integrität

Agilität für Business bieten

- Dynamische Data Center & Desktops
- Erhöhung der Reaktionszeiten
- Compliance

Microsoft

Themenblöcke Sicherheit

Schutz gegen Viren und Schadsoftware

- Viren, Spyware und Würmer
- Botnetze und Rootkits
- Phishing und Betrugsfälle

Geschäfts-praktiken

- Einhaltung von Vorschriften
- Entwicklung & Implementierung von Sicherheitsrichtlinien
- Reporting und Haftungsfragen

Implementierung grundlegenden Schutzes

- Identitätsmanagement und Zugriffssteuerung
- Verwalten von Remote Access
- Sicherheitsrisiko durch nicht verwaltete PCs

Sicherheits-Management

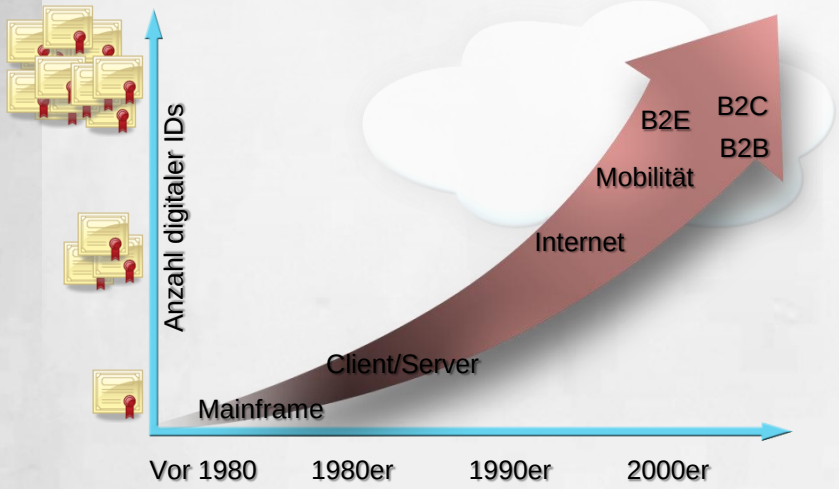
- Einspielen von Sicherheits-Updates
- Systemidentifizierung, Konfiguration
- Durchsetzen von Sicherheitsrichtlinien

Microsoft

Bedrohungstrends

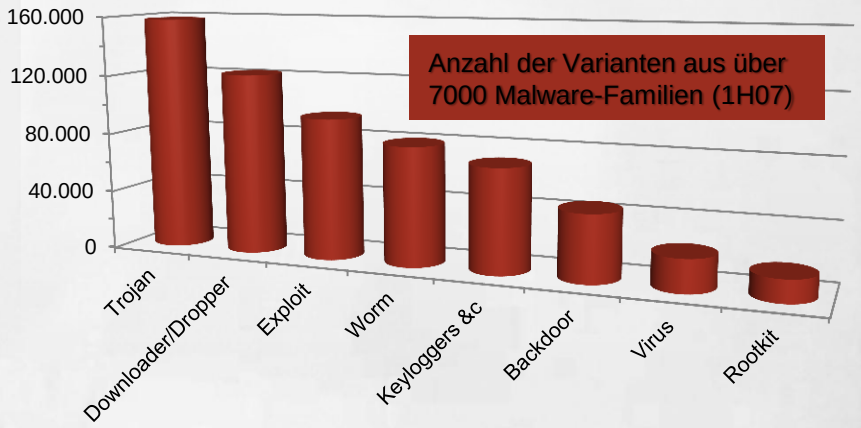
Exponenzielles Wachstum der IDs

Herausforderung der Identitäts- und Zugriffsmanagement



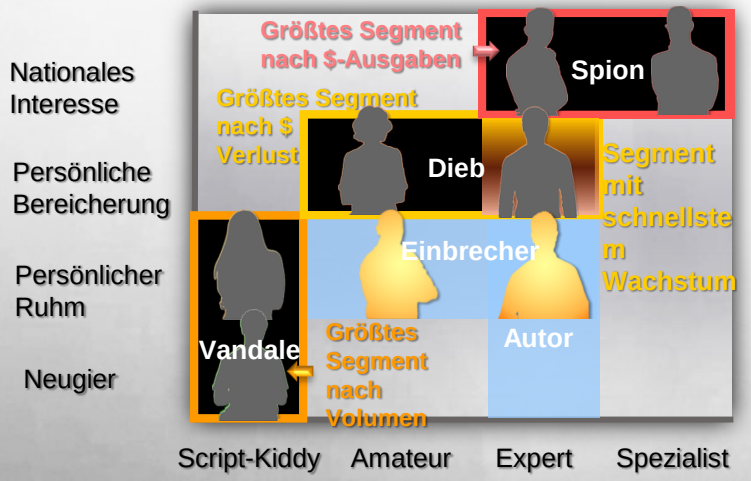
Zunehmend raffinierte Malware

Anti-Malware reicht nicht mehr aus



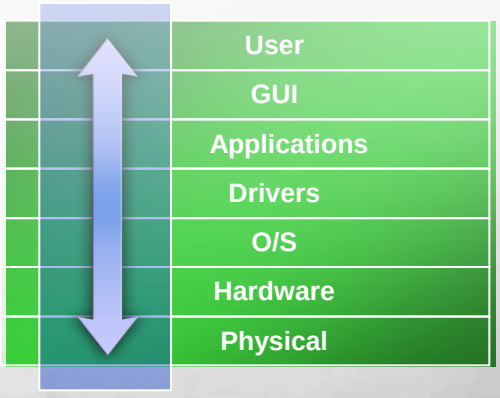
Qeulle: ***Microsoft Security Intelligence Report (Januar – Juni 2007)***

Verbrechen nehmen zu



Zunehmend raffinierte Angriff

Traditionelle Verteidungsmethoden sind nicht mehr wirksam

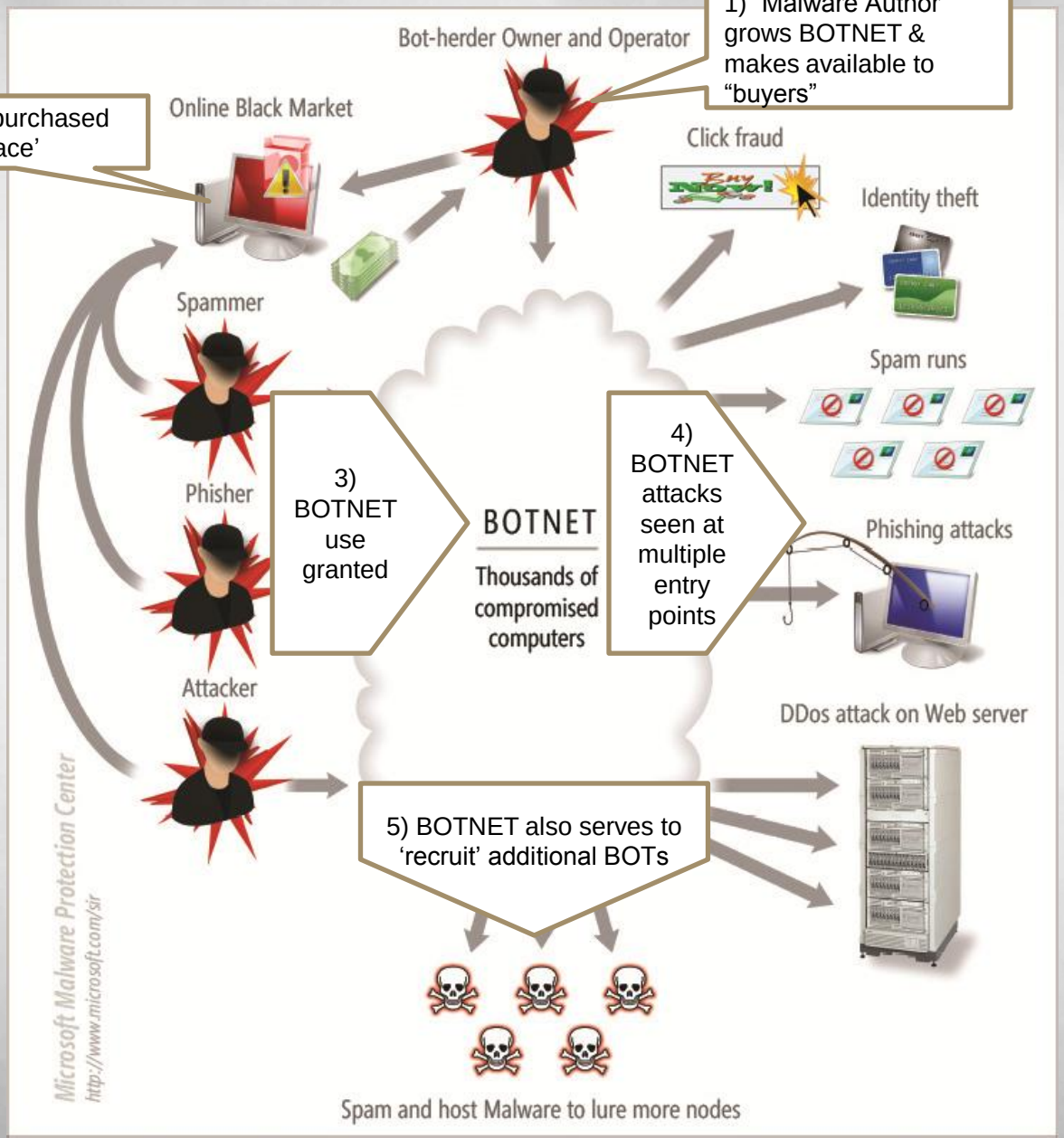


Bespiele

- Spyware
- Rootkits
- Angriffe auf Anwendungen
- Phishing/Social-Engineering

Microsoft

Das Bedrohungs-Ökosystem



Was nun?

Die entscheidenden Elemente …

Microsoft

..und Ihr Zusammenspiel.

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

Microsoft

Struktur und Verantwortung: ISMS – Information Security Management System

Kontrollmechanismen um Wirksamkeit von Sicherheits-maßnahmen nachvollziehbar und nachweisbar machen zu können.

Sicherheitsleitlinie, Ziele

1. Übernahme der Gesamtverantwortung
2. Integrierte Sicherheit
3. Sicherheit steuern und aufrechterhalten
4. Erreichbare Ziele setzten
5. Kosten Nutzen abwägen
6. Vorbildfunktion

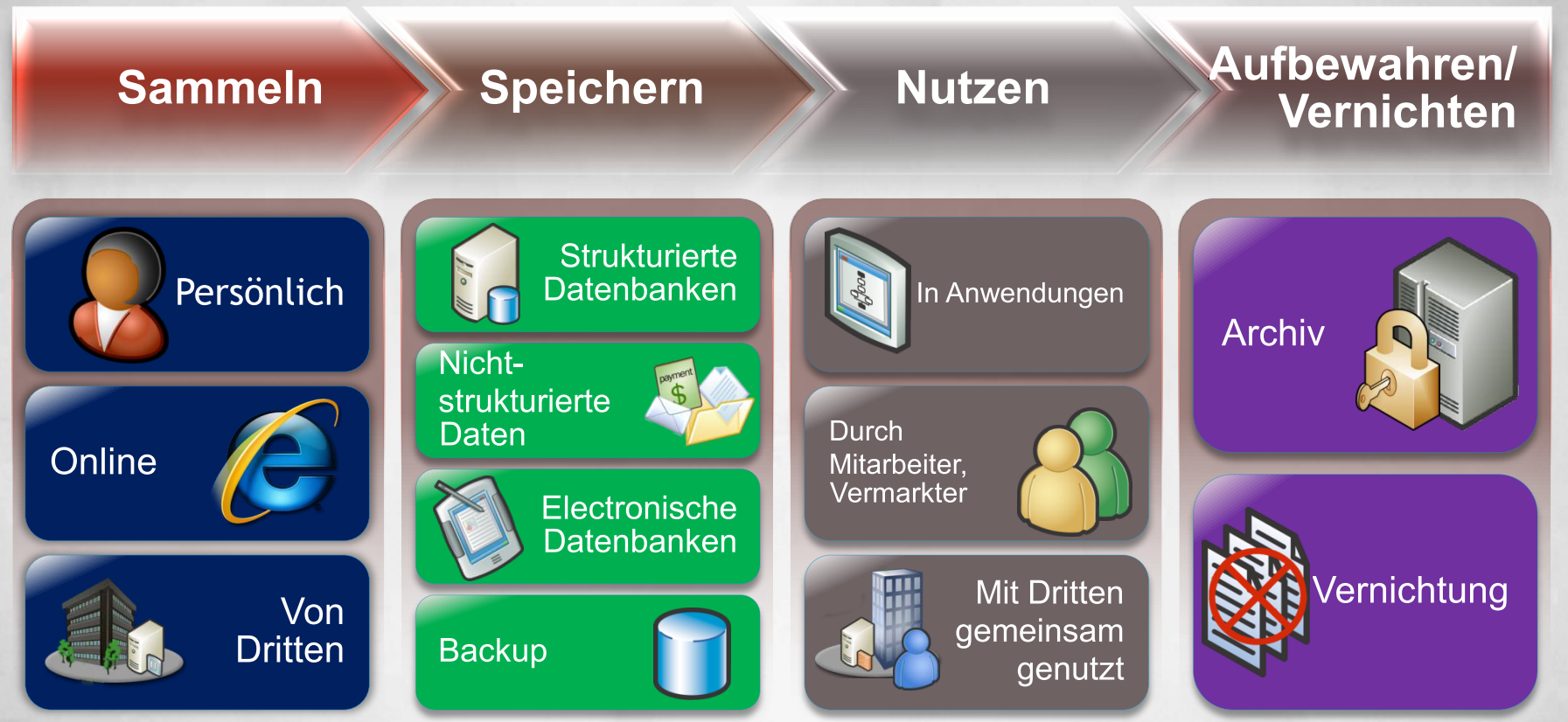
Finanziell, Personnel, Zeit

Bewusstseins, Wertevorstellung, Skills

Berichten
Informieren
Dokumentieren

vgl. BSI Standard 100-1

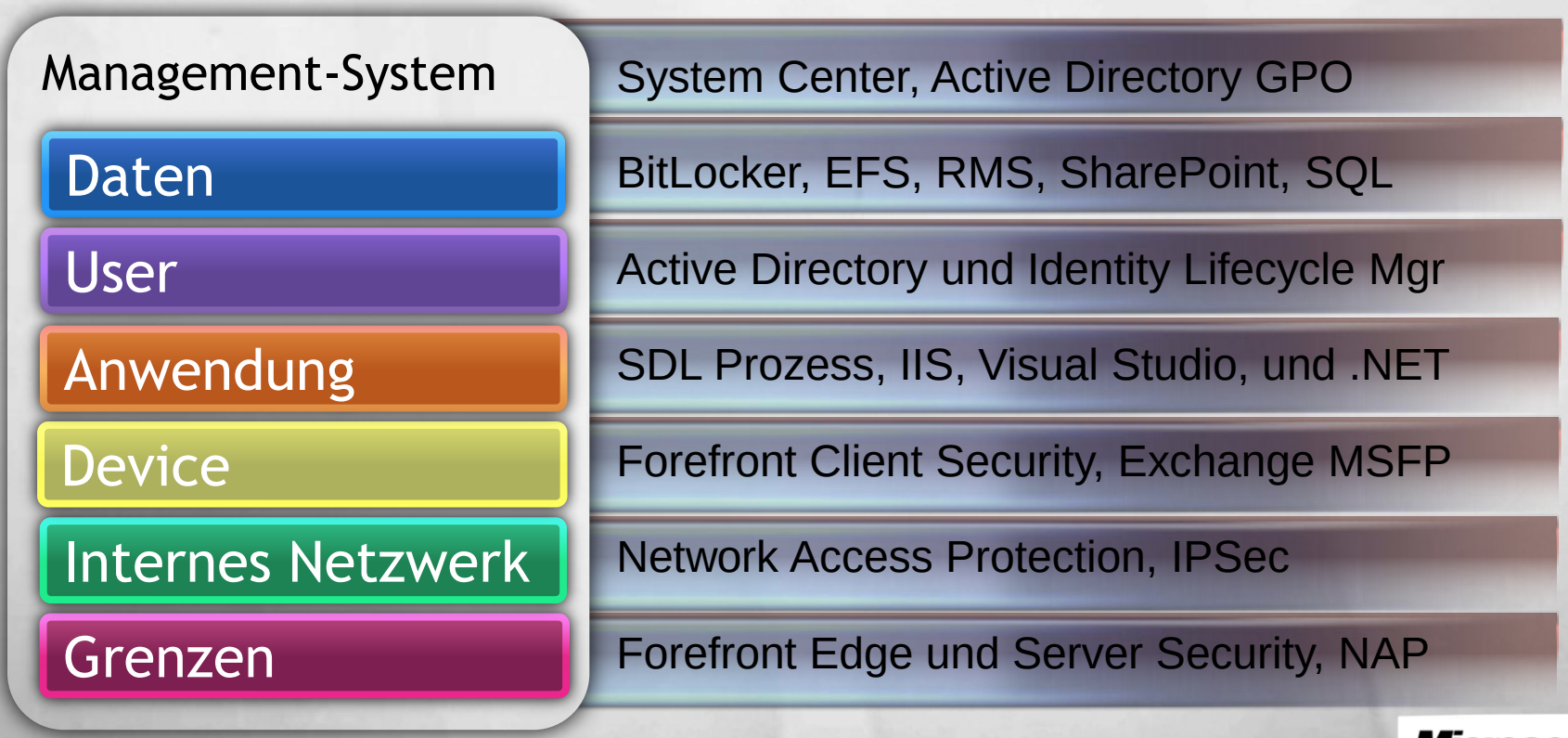
Vertraulichkeit und GRC



Interoperabilität des Sicherheits-Stack

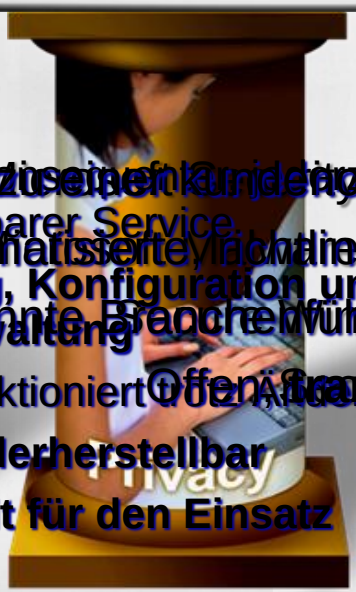
Integrierte Sicherheit vereinfacht die Abwehr beim Einsatz in einer Architektur mit mutliplen Verteidungsebenen

Aufnahme von offenen Standards ermöglicht die Integration über Plattformgrenzen



Microsoft

Trustworthy Computing



Voraussagbarer Service

Automatisierte, richtlinienbasierte Lösungen

Einfache **Wartung, Konfiguration und Verwaltung**

Anerkannte Branchenführer

Widerstandsfähig, funktioniert trotz Änderungen

Offen, transparent

Leicht wiederherstellbar

Bewährt, bereit für den Einsatz

Richtlinien für die Entwicklung von Software und Services

Weltklasse-Partner

Microsoft Data Governance Framework

Verwaltung und Schutz von persönlichen Daten

2002

- TWC angekündigt
- SDL beginnt
- Sicher gegen Angriffe
- Schützt die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen

2003

- Windows Server 2003

2004

- Windows XP SP2 DSI veröffentlicht
- Lösungen zum Schutz der Vertraulichkeit erstellen
- Schutz für Ihre Unternehmensdaten
- Schutz für die Privatsphäre

2005

- SQL Server 2005
- Visual Studio 2005
- Windows Server 2003 SP1
- Malicious SW Removal Tool
- Microsoft Online Crash Analysis
- Engineering Excellence Training und Richtlinien
- Microsoft Online Services mit hoher Zuverlässigkeit in multiplen Datacentern
- Vendor Engagement und Windows Hardware Quality Lab
- Business Continuity explizit für erzwungene Führung konzipiert

2006

- Windows Defender
- Windows Live OneCare

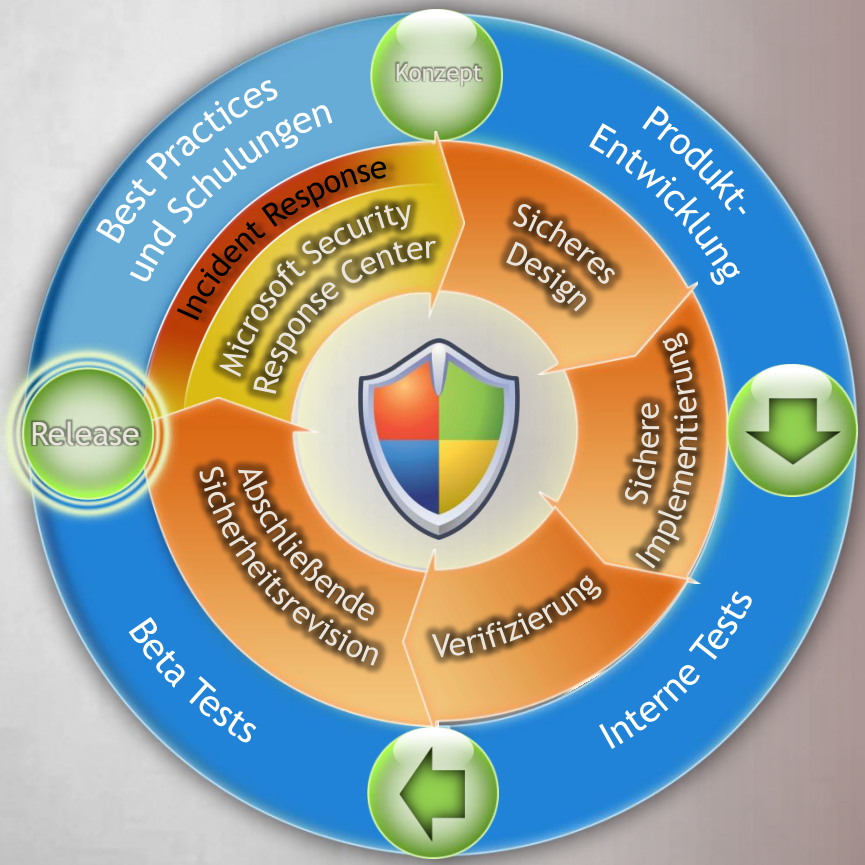
2007

- Windows Vista
- Office 2007
- Forefront

2008

- Interop Vendor Alliance
- Open Source Software Lab
- Transparente Praktiken (SDL, Codeplex, usw.)
- Windows Server 2008
- SQL Server 2008

Die Microsoft Sicherheits-Entwicklungslebenszyklus



Ziele

Microsoft-Kunden schützen durch

Reduzierung der **Anzahl** der Schwachstellen

Reduzierung der **Schwere** der Schwachstellen

Wichtigste Prinzipien

Zwingender jedoch auch praktischer Ansatz

Proaktiv – nicht nur “nach Bugs suchen”

Sicherheitsprobleme in einer frühen Phase ausschließen

Sicher durch Design

Microsoft

Die Integration der Sicherheit in Software und Kultur

Bei Microsoft glauben wir, dass zur Bereitstellung sicherer Software folgendes gehört:

Engagement auf Managementebene → SDL Richtlinie bei Microsoft seit 2004

Training	Anforderungen	Design	Implementierung	Verifizierung	Release	Response
• Core training	• Analyse der Bedrohung für die Sicherheit und Vertraulichkeit • Qualitätsziele definieren	• Modellieren der Bedrohungen • Analyse der Angriffsfläche	• Tools definieren • Verboten Funktionen erzwingen • Statische Analyse	• Dynamisches/ Fuzz-Testing • Bedrohungsmodelle / Angriffsfläche verifizieren	• Response-Plan • Abschließende Sicherheitsrevision • Release-Archiv	• Response ausführen

Schulung

Technologie und Prozess

Haftungsfragen

Laufende Prozessverbesserungen → 6-Monatszyklus

Microsoft® Visual Studio®

Optimierungsmodell für die Kern- Infrastruktur

IO nutzen, um Ihre Sicherheitsinfrastruktur zu verstehen

Basis	Standardisiert	Rationalisiert	Dynamisch
Kein gemeinsames Identitätsmanagement-modell	Identitäts- und Zugriffsmanagement		Föderiertes Identitäts-management über org. und Plattformgrenzen
Keine Standards für Desktops bzw. Server, viele Images, keine Management-Standards	Desktop-, Device- und Servermanagement		Automatisertes IT-Management, dynamische Ressourcennutzung
Keine Netzwerk- und Sicherheitsstandards	Sicherheit und Netzwerke		Automatisiertes Sicherheits- und Netzwerkmanagement
Adhoc-Schutz kritischer Daten	Datenschutz und Wiederherstellung		Datenschutz zwischen Endpunkten, Disaster-Recovery
Adhoc, reaktiv	IT- und Sicherheitsprozess		Proaktiv, Optimierung von Kosten & Leistung, End-to-End-Service & Richtlinienmanagement

Microsoft

Fortschritte in der Sicherheit und Vertraulichkeit

SDL und SD3

- Security Development Lifecycle process
  - Engineered for security
  - Modellierung von Bedrohungen im Design
- SD3
  - Secure by Design (sicheres Design)
  - Secure by Default (standardmäßig sicher)
  - Secure In Deployment (sicher im Einsatz)
- Automatisierte Patch- und Update-Services

Multiple Verteidigungslinien

- Malware-Beispiel
  - Verbraucherschulungen
  - Gesetze
  - Firewalls
  - Antiviren-Produkte
  - Antispyware-Produkte
  - Malicious Software Removal Tool
  - Speicher-Management (ASLR)
  - Gesetzeshüter

Bekämpfung der Bedrohungen

- Microsoft Security Response Center (MSRC)
- Microsoft Malware Protection Center (MMPC)
- Windows Live OneCare und Forefront Client Security, über Microsoft Malware Protection Center
- SPAM (Sender ID, Phishing Filters)
- Network Access Protection (NAP/NAC)

Microsoft

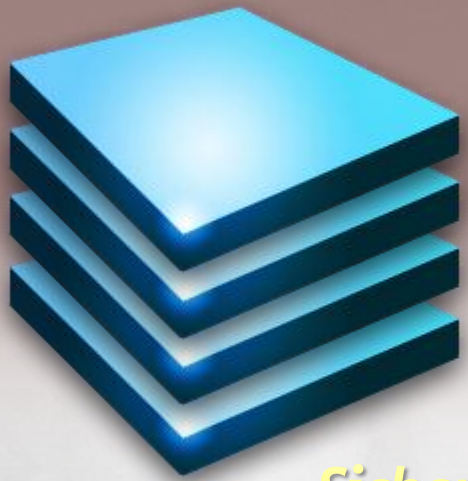
Aufbau eines “Trusted Stack”

Kritische Sicherheitskomponenten

“I+4A”

- Beanspruchte Identität
- Authentifizierung
- Autorisierung
- Zugriffssteuerungsmechanismen
- Revision

Trusted Stack



- Vertrauenswürdige Daten
- Vertrauenswürdige Menschen
- Vertrauenswürdige Software
- Vertrauenswürdige Hardware

Sichere Grundlage

Integrierter Schutz

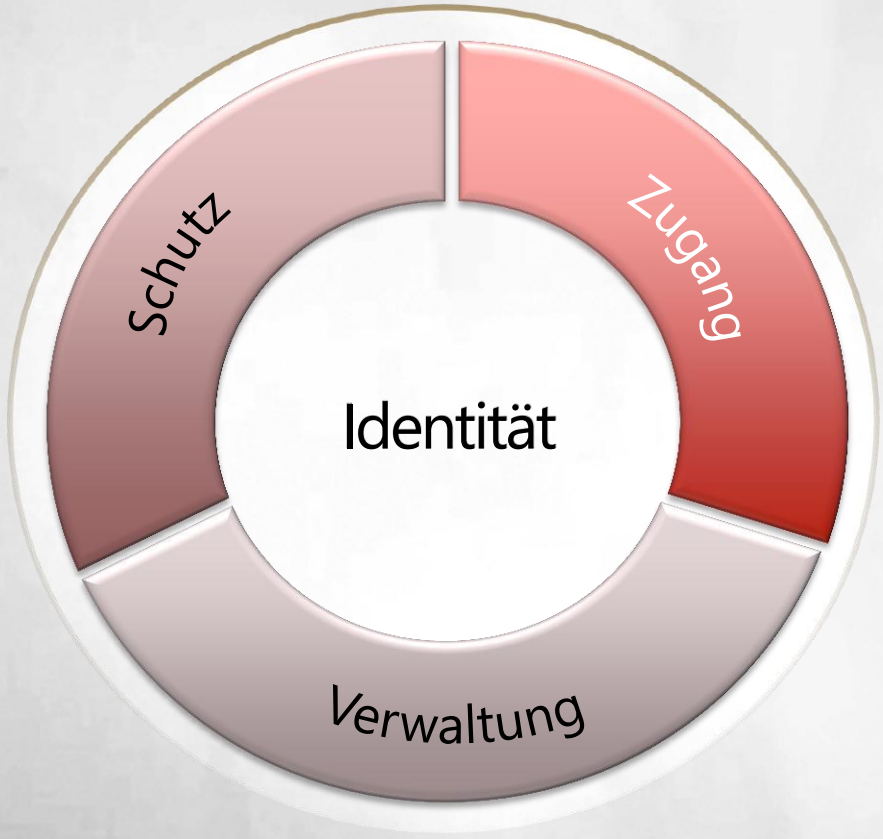
- SDL und SD3
- Multiple Verteidig-ungslinien
- Bekämpfung der Bedrohungen

Microsoft

Der Ansatz von Microsoft

Microsoft

Unser Ansatz: **Microsoft Business Ready** Security



Sicherheits- und Identitäts-Lösungen bilden eine untrennbare Einheit

Microsoft

Themenbereiche für System/Service Management

Microsoft

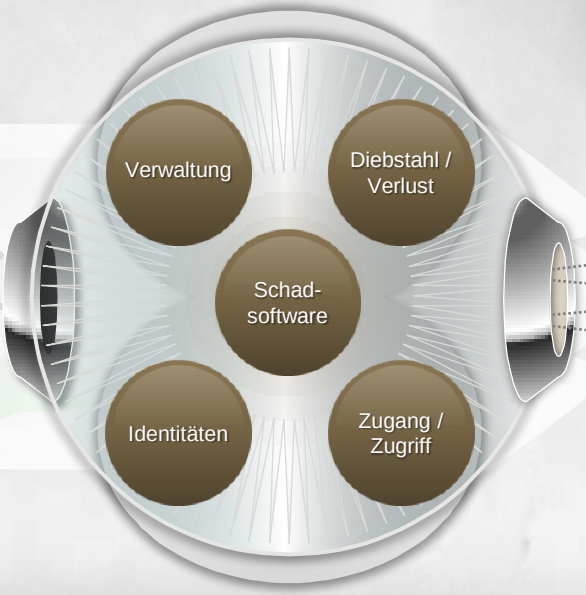
Lösungsansatz

Business Ready Security

Kommunikationsicherheit

Schutz der Informationen

Absicherung von Endgeräten



Sichere Kommunikation

Sichere Zusammenarbeit

Sichere Endgeräte

Warum nicht verschiedene Lösungen bzw. Hersteller einsetzen?

Schwierig zu integrieren und hohe Betriebskosten	• Nutzung unterschiedlicher Architekturen und Standards • Inkonsistente Prozesse zur Verteilung und Betrieb
Führt häufig zur Über-Lizensierung	• Sicherheits-Suiten haben teilweise funktionale Überlappungen • Unvereinbare Lizenzierungsmechanismen
Unterschiedliche Support- und Helpdesk-Prozesse	• Hersteller weisen sich gegenseitig Fehler bei Interop-Problemen zu • Überschneidungen bei Support-Verträgen erzeugen unnötige Kosten

Microsoft

Microsoft: Business Ready Security

Microsoft® Forefront™
Business Ready Security

1. Integrierter Schutz über die gesamte Infrastruktur
2. Komfortabler Zugriff von jedem Ort – bei gleichzeitigem umfassenden Schutz
3. Umsetzung rechtlicher Anforderungen und Transparenz der Sicherheit für den Endanwender

Sichere Kommunikation

Sichere Zusammenarbeit

Endgeräte-Sicherheit

Schutz der Informationen

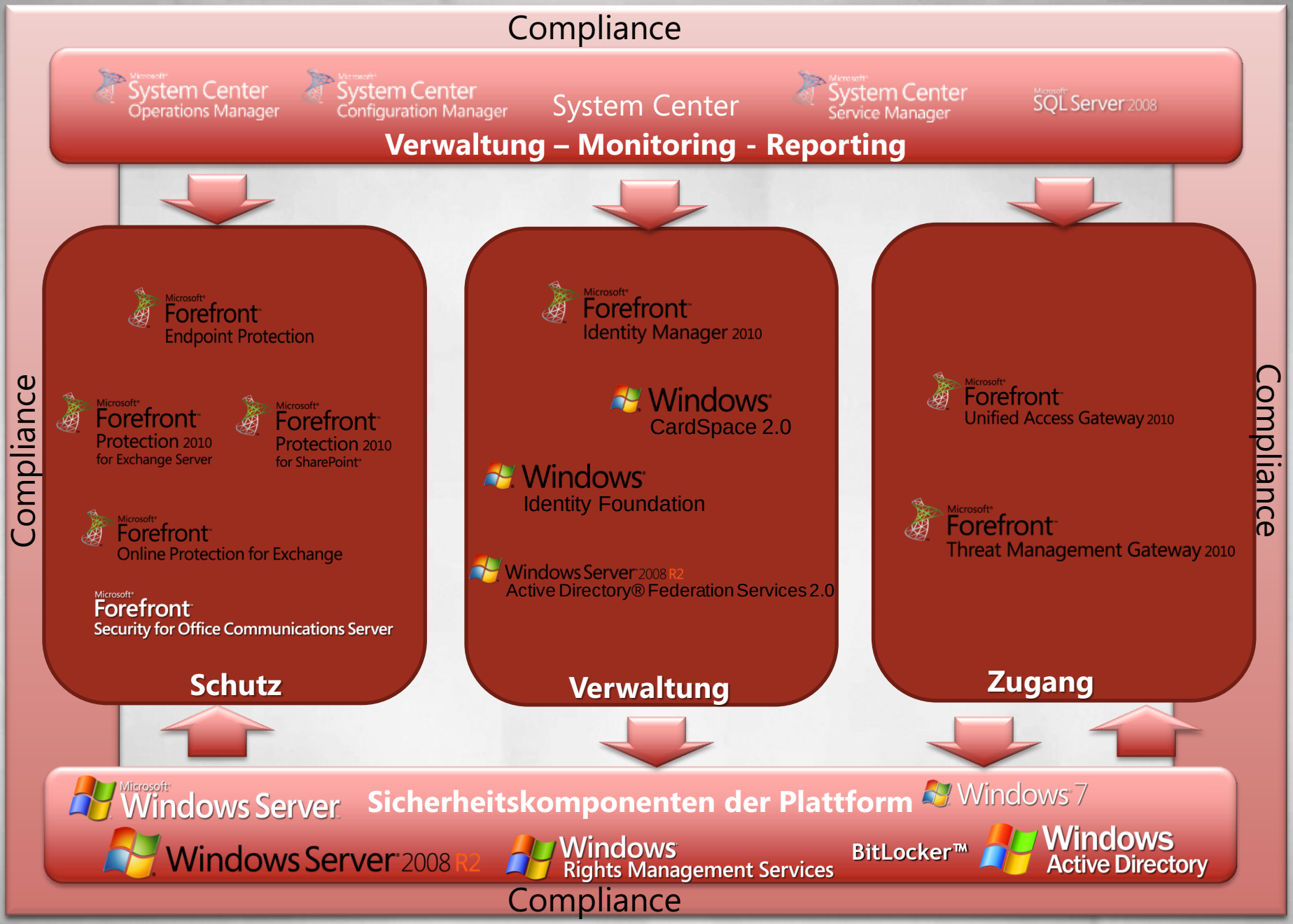
Identitäts- und Zugangs-Verwaltung

Microsoft

Abgrenzung Produkte vs. eingebaute Funktionalitäten

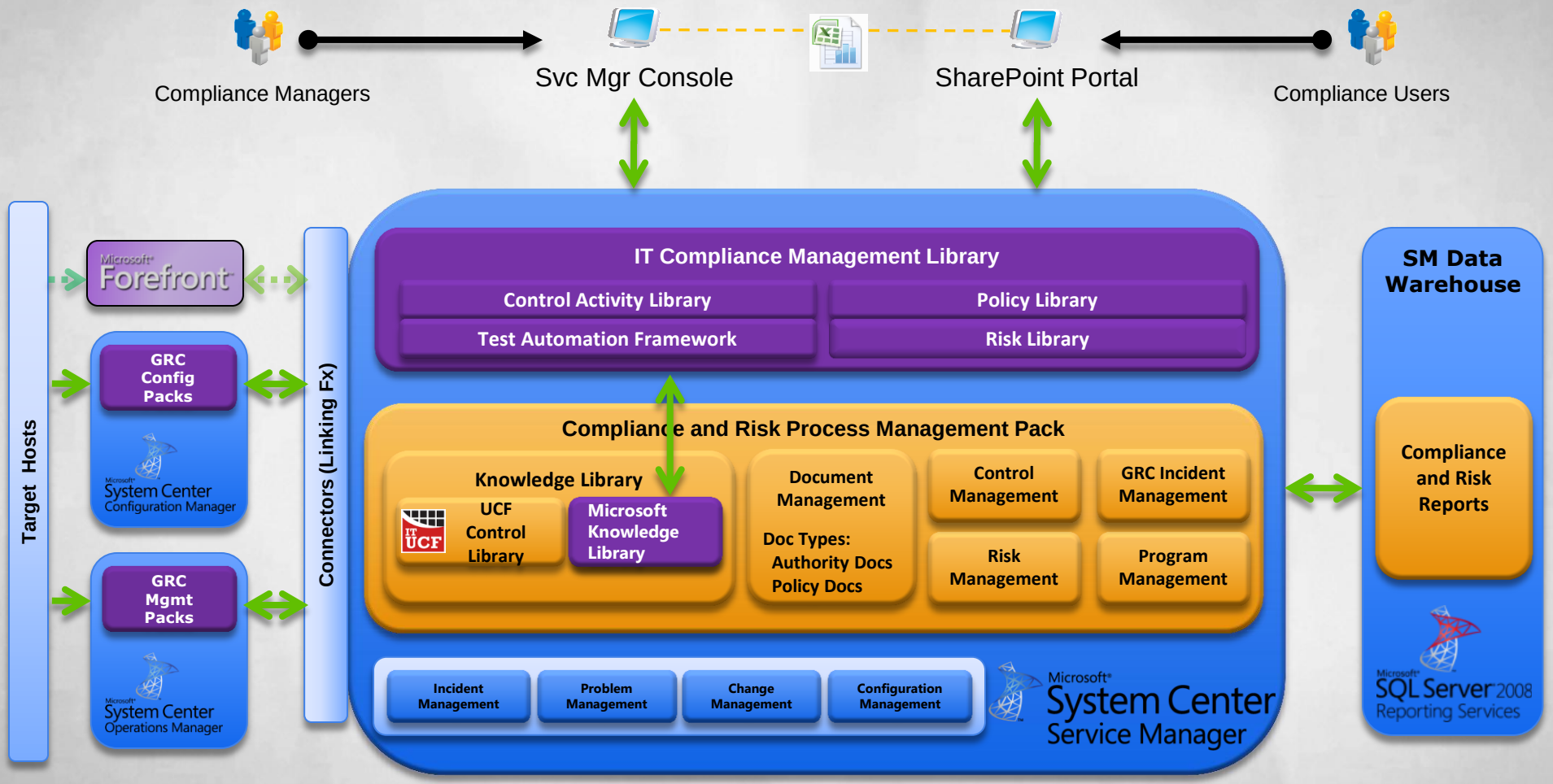
	Microsoft® Forefront™	Sicherheits-funktionalitäten
 Schad-Software Schutz	Forefront AV-Lösungen u.a. für den Client, Exchange, SharePoint	u.a. Windows Defender, Internet Explorer Protected Mode
 Sicherer Zugang & Netzwerk Schutz	Firewalll und VPN-Lösungen wie Threat Management Gateway und Unified Access Gateway	u.a. Network Access Protection (NAP), Direct Access, User Account Control
 Informations-Sicherheit	AD Rights Management Services (RMS) mit Integration in SharePoint, Exchange, Office	u.a. BitLocker, EFS, BitLocker to Go, USB Device Control
 Identitäts- & Sicherheits-Verwaltung	Dazu zählt Forefront Identity Manager	u.a. Active Directory und PKI Management in Windows Server

Microsoft


Compliance
System Center
Operations Manager
System Center
Configuration Manager
System Center
System Center
Service Manager
SQL Server 2008
Verwaltung – Monitoring - Reporting
Compliance
Forefront
Endpoint Protection
Forefront
Protection 2010
for Exchange Server
Forefront
Protection 2010
for SharePoint
Forefront
Online Protection for Exchange
Forefront
Security for Office Communications Server
Schutz
Forefront
Identity Manager 2010
Windows
CardSpace 2.0
Windows
Identity Foundation
Windows Server 2008 R2
Active Directory® Federation Services 2.0
Verwaltung
Forefront
Unified Access Gateway 2010
Forefront
Threat Management Gateway 2010
Zugang
Compliance
Windows Server
Sicherheitskomponenten der Plattform
Windows 7
Windows Server 2008 R2
Windows
Rights Management Services
BitLocker™
Windows
Active Directory
Compliance

Wie genau spielt hier Compliance mit?

GRC Management Suite Architecture



Microsoft

Unified Compliance Framework

Microsoft Compliance Framework

Microsoft Compliance Framework Maps GRC Authority Docs (Regulatory, Standards, Guidance) to Control Objectives

Seeded with IP from UCF – will be maintained by them

293 Laws and Standards, 30 Best practices

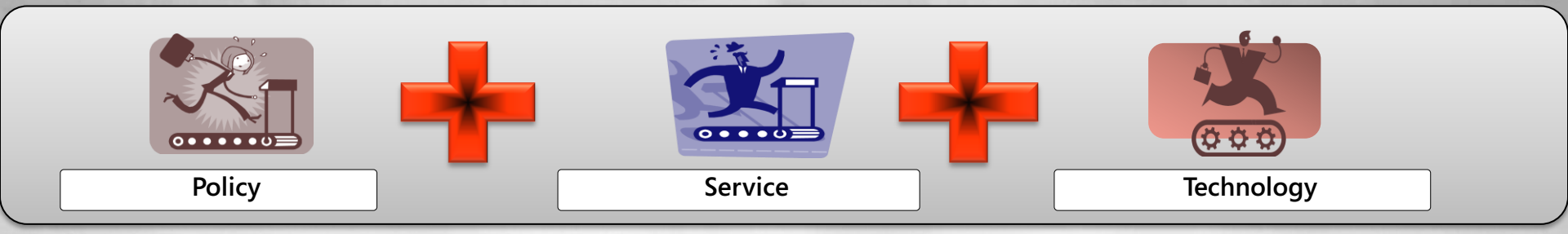
Represents 21 Countries

Mapped to 2500 Unique Control Objectives in English organized in a tree

Monitoring and measurement	00636
Establishing overall monitoring and logging operations	00637
Operationalizing key monitoring and logging concepts	00638
Measurement	00639
Traceability	00640
Synchronize system clocks	1340
Log user identification	1334

You don't have to worry about thousands of regulations, interpreting them or de-duplicating between them !

Microsoft



GRC Authority Docs
(Requirements)

Harmonized Framework

Objectives

CONTROL OBJECTIVES

Technologies

System Center | WS 2008 | Windows 7

Technical Means

Control Activities

Validation Infrastructure

Test Automation
Workflows – CMDB – Data Warehouse

FOREFRONT | OPERATIONS MANAGER | CONFIGURATION MANAGER | ACTIVE DIRECTORY

Microsoft

CA: Establish System Notification and Banner Warnings

GRC
Program Manager

Control Activity

- Implement Procedure
- Determine Values
- Validate Settings
- Detect Failure
- Record Result
- Take Action

GPO

Windows Server 2008 R2

Workflow

Service Manager
CMDB

Failure

Dashboard

Corrective Actions

GRC Reports | GRC Incident/ Issue | GRC Problem

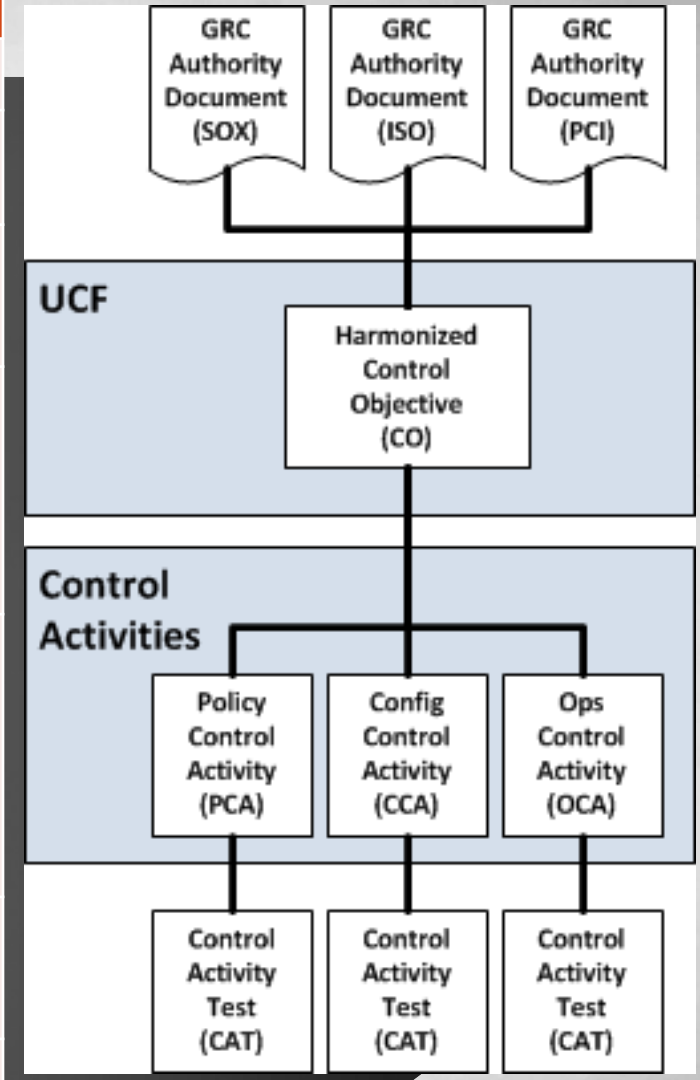
Actions

Operations Engineer

Microsoft

GRC Taxonomy

Terminology	Example
GRC Authority Document	**SOX, HIPAA, PCI, EUDPD, ISO, GLBA**
Unified Compliance Framework	A hierarchical organization of the smallest set of non-duplicated business requirements from ~350 world-wide GRC authority documents.
Control Objective (CO)	A harmonized statement of expectations from GRC Authority Documents containing requirements. *Ex:* **CO 04544: Synchronize system clocks**
Control Activity (CA)	Microsoft interpretations of CO requirements as applied to our platform, including the goal to be achieved and best practice based activities on how to achieve it. *Ex:* **CCA: Configure Windows Time Service** **OCA: Monitor Windows Time Service** **PCA: Network Time Protocol Policy**
Test Automation	Automated workflow or manual assertion that apply GRC based-business intelligence and program scope to validate whether or not the goal of the associated CA has been achieved. *Ex:* **• Ensure the Windows Time Service is running** **• Ensure the NtpClient has an accurate source of time** **• Ensure the required policy has been specified and remains available**
Library	Compliance information stored as templates which can be instantiated with specific values and parameters in a program *Ex:* **IT Compliance Management Library.XML**
Program	Logical grouping containing compliance data (COs/CAs), automated tests, and applicable scope of assets *Ex:* **East Coast Sarbanes Oxley Program**



Microsoft

Produkte Rund um Compliance

SCCM Grundschutzmodul

SC Service Manager Risk & Compliance Modul

http://www.microsoft.com/systemcenter/en/us/service-manager.aspx

http://technet.microsoft.com/en-us/evalcenter/ee348897.aspx

http://edge.technet.com/Media/Managing-Compliance-with-System-Center-Service-Manager-2010/

http://www.microsoft.com/systemcenter/en/us/default.aspx

Compliance Manager

http://technet.microsoft.com/de-de/library/cc677002(en-us).aspx

http://go.microsoft.com/fwlink/?LinkId=182512

Zum Schluss…

Microsoft

Weiterführende Informationen

- http://www.forefront.de
- http://www.microsoft.com/forefront

Microsoft Security Essentials (MSE)
www.microsoft.de/mse

- Speziell für Heimanwender konzipierte, kostenfreie Antiviren- Software, die PCs mit legitimen Windows-Versionen vor Viren, Würmern und anderer Malware schützt. (Jetzt bis zu 10 PCs)

- Verfügbar für Windows 7, Windows Vista und Windows XP mit Service Pack 2

Microsoft

Microsoft®

Your potential. Our passion.™

Microsoft®