Sicherheit in Intranetzen

Thomas J. Wilke

Vortag am TIK der ETH Zürich

Zürich, den 27.11.2000

Gliederung

- Begriffsbestimmung „Sicherheit“
- Komplexität moderner IT-Infrastrukturen
- Bedrohungsklassen komplexer IT-Infrastrukturen
- Anforderungen an Sicherungsmechanismen
- Gegenwärtige Verfahren zur Absicherung
- Alternative Ansätze zur Absicherung

Begriffsbestimmung „Sicherheit“

- **Abstrakte Definition**

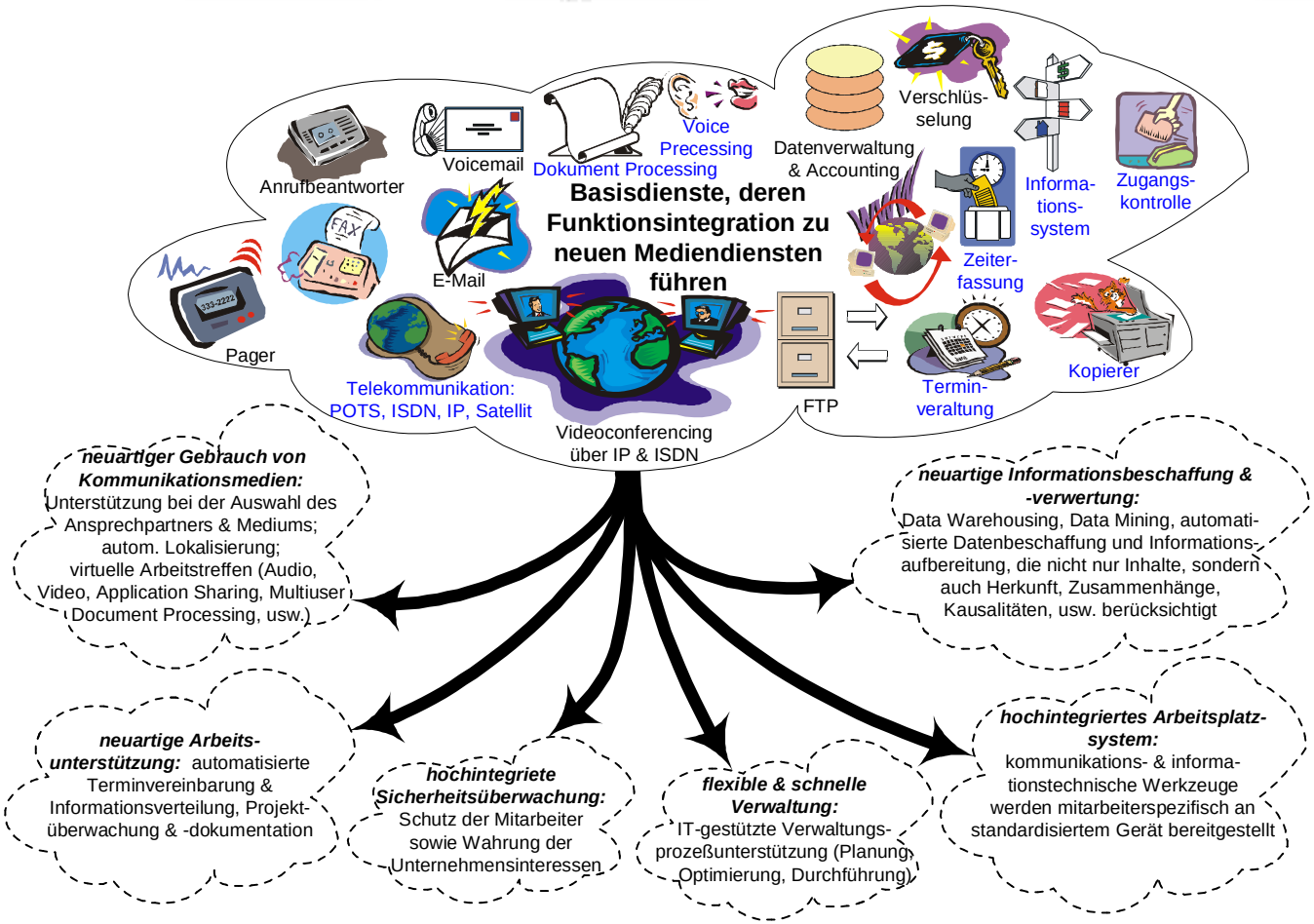
  Sicherheit ist ein relatives Maß, das angibt, wie wahrscheinlich ein Ereignis (oder eine Gruppe von Ereignissen) in einem definierten Umfeld eintritt.

- **Elementbezogene Definition**

  Sicherheit ist ein Maß für die Schutzbedürftigkeit von Objekten oder Subjekten in einem definierten Umfeld. Die Schutzbedürftigkeit korreliert mit der (wirtschaftlichen) Bedeutung, die dem Objekt oder Subjekt im jeweiligen Umfeld zugeschrieben wird.

Komplexität moderner IT-Infrastrukturen:

Funktionsanforderung für die innerbetriebliche Nutzung



Komplexität moderner IT-Infrastrukturen:
Betriebsprozeßmodell

- Betriebsprozeßspezifische-IT-Ebene

  Beschreibung der Verarbeitung von Betriebsprozessen:

  Workflow ⇔ elektronische Abbildung und Bearbeitung

- Basis-IT-Ebene

  Beschreibung der Basisdienste:

  Funktionsbeschreibung ⇔ systemtechnische Realisierung

- Elementar-IT-Ebene

  Beschreibung der rechen- und übertragungstechnischen Grundlage der IT-Infrastruktur

Bedrohungsklassen komplexer IT-Infrastrukturen:

- höhere Gewalt
- technisches Versagen
- Organisationsmängel
- unbeabsichtigtes Fehlverhalten
- Angriffe von innen: Betriebsangehörige
- Angriffe von außen: Betriebsfremde
- kooperierende Angriffe von innen und außen
- Kombinationen aus den genannten Klassen

Bedrohungsklassen komplexer IT-Infrastrukturen:
Wirkungsziele

- unberechtigter Zugang zu Daten und/oder Systemen
- Datenmanipulation
- Funktionsbeeinflussung technischer Systeme
- Manipulation von Menschen
- Vorspiegelung einer falschen Identität
- Kombination aus den genannten Wirkungen

Anforderungen an Sicherungsmechanismen:

qualitative Anforderungen

- Sicherstellung des befugten Zugriffs auf Subjekte und Objekte im Intranetz
  Identifikation, Authentifikation, DAC, MAC
- Sicherstellung der Kommunikation in Intranetzen
  Authentizität, Integrität, Vertraulichkeit, Verbindlichkeit
- Sicherstellung der Verfügbarkeit und Korrektheit vitaler Funktionen
  Personal, Situationserkennung und -handhabung, Installations-management
- Vermeidung von verdeckten Kanälen
  Identifikation, Authentifikation,
- Rechtsverwertbarkeit
  Accounting, Kommunikationsinhalte, Auditing von Vorgängen

Anforderungen an Sicherungsmechanismen:

funktionale Anforderungen

- sichere Bereiche
  Schutzbereiche, in denen die Funktion bzw. Darstellung von Subjekten bzw. Objekten nicht unterlaufen werden kann.
- einheitliche Schnittstellen
  zwischen Subjekt ↔ Objekt sowie Subjekt ↔ Subjekt, die eine Zugangskontrolle, Ablaufüberwachung und Ablaufprotokollierung bereitstellen.
- Dokumentation
  abstraktionsadäquate Beschreibung des Ist-Zustandes der Elemente
- Überwachung
  zeitnahe Auswertung des Ist-Zustandes
- durchgängige Durchsetzung einer Sicherheitspolitik
  über verschiedene Beschreibungsebenen hinweg

Gegenwärtige Verfahren zur Absicherung

- Identifikation, Authentifikation ⇒ Kerberos, PKI, ...
- Datentransportabsicherung ⇒ SSL, PPTP, IPSec,...
- Anwendungsspezifische Absicherung ⇒ HTTPS, SHTTP, MIME/S, PGP, SSH, SFTP
- Absicherung von transaktions-orientierten Anwendungen ⇒ SET, HBCI, ...
- aktive Ausschaltung „uner-wünschter Objekte“ ⇒ Virenscanner & Application-Firewallsysteme
- Netzwerkmanagement ⇒ SMNP v3, prop. Managementnetz
- proprietäre Sicherheitspolitiken ⇒ NT, Unix, VCAM, Firewall-systeme, anwend.-spez. Politiken

Alternative Ansätze zur Absicherung

- Etablierung von „sicheren Bereichen“
- Verminderung der Komplexität (Reduzierung der Anzahl der möglichen Beziehungen)
- durchgängige Beschreibung einer Sicherheitspolitik für alle Abstraktionsebenen
- durchgängige Durchsetzung einer Sicherheitspolitik mittels transparenter Mechanismen
- aktive Ausschaltungen fremder Subjekte

Gegenüberstellung der Ansätze

gegenwärtige Ansätze		alternative Ansätze
erprobte Funktionalität	⇔	keine Erfahrungswerte
überschaubare Komplexität	⇔	hohe Komplexität
voneinander abgegrenzte Prbl.	⇔	integrative Problembewältigung
Geringe Unterstützung von Systemveränderungen	⇔	Unterstützung dynamischer Systemveränderungen
begrenzte, homogene Unterstützung heterogener Strukturen	⇔	homogene Unterstützung heterogener Strukturen
* / *	⇔	Möglichkeit der Implementierung neuer Wirkungsmechanismen, die sich über unterschiedliche Abstraktionsebenen erstrecken