IT-SECURITY - Forum #2

Identitätsmanagement Begriffe und Konzepte

Dr. Hannes P. Lubich
IT Security Strategist
Computer Associates Schweiz

IT-SECURITY - Forum #2

Begriffsbildung

- **Identität**: Überprüfbares Set von Attributen und zugehörigen Werten, die eine Einheit (eine Person, ein System, einen Prozess) beschreiben. Attribut und Wert bilden dabei einen eindeutigen Namen für eine Einheit.
  - die Einzigartigkeit des Namens bzw. Attribut/Wert-Paares gilt nur in einem definierten Kontext (Staat, Firma, etc.)
  - eine Einheit kann in verschiedenen Umgebungen durchaus verschiedene Namen annehmen
  - die Identität unter Kontrolle der Einheit kann an Agenten (Drittparteien, Software) delegiert sein.

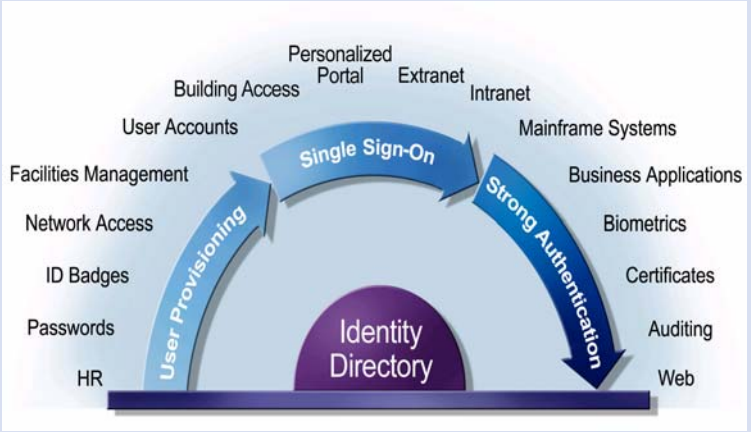
IT-SECURITY - Forum #2

Teilschritte des Identitäts-Mgmt

- **Identifizierung**: Prozess des Erkennens einer Einheit aufgrund der Identität
- **Authentifizierung**: Bestätigung, dass eine Einheit die behauptete Einheit ist (beim Empfänger).
- **Authentisierung**: Zufügen einer nicht nachträglich änderbaren oder verfälschbaren Information zu Nutzinformation durch den Sender (z.B. Prüfsumme oder digitale Signatur) (beim Sender)
- **Autorisierung**: Prozess, einem Subjekt oder Akteur basierend auf einer erfolgreichen Authentifizierung Zugriffsrechte zuzuweisen

IT-SECURITY - Forum #2

Identitäts-Management Zyklus



IT-SECURITY - Forum #2

Identitäts-Management Architekturen

Zentralisiert: Vergabe von global gültigen, eindeutigen Identitäten

Dezentral: Jeder vergibt und verwaltet Identitäten in „seinem“ Kontext individuell

Föderativ: Keine einheitlichen Identitäten, aber Vernetzung von Identitäten

IT-SECURITY - Forum #2

Einsatzgebiete

Rechtverbindliche, nachvollziehbare, vertrauenswürdige und geschützte Prozessketten für:

- B2B (Verträge, Zulieferungen, Zahlungen, ...)
- B2C (Bestellung, Auskunft, Lizenzierung, e-Banking, ...)
- P2P (Privatverkäufe, Auktionen, ...)
- G2C (Interaktion zwischen Regierung/Behörden und Bürgern)

Angebot „für jedermann“ als Basistechnologie / Basisdienst, z.B. gebündelt mit populären Betriebssystem und Software-Anwendungen

Aufbau neuer Geschäftsprozesse und Nutzungsmodelle auf einer vertrauenswürdigen Basis, z.B. Agenten (Personen, Software), die für Akteure Dinge im Auftrag erledigen, dabei Teilaufträge an Dritte weiterreichen und die Teilergebnisse konsolidieren.

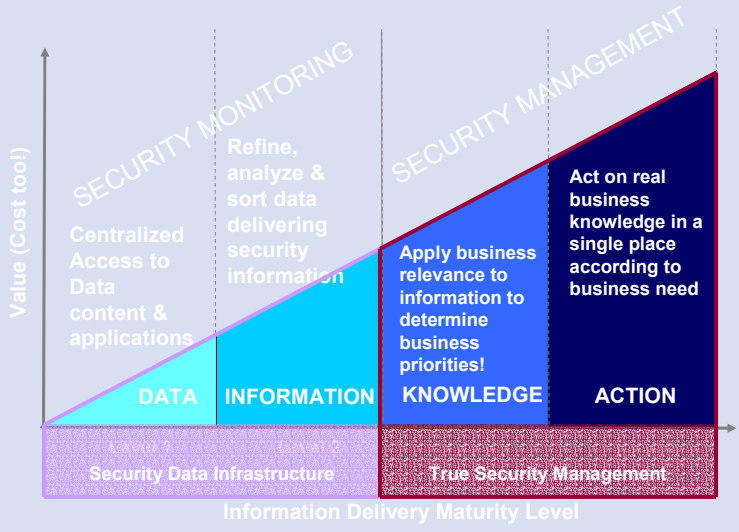
IT-SECURITY - Forum #2

Risiken

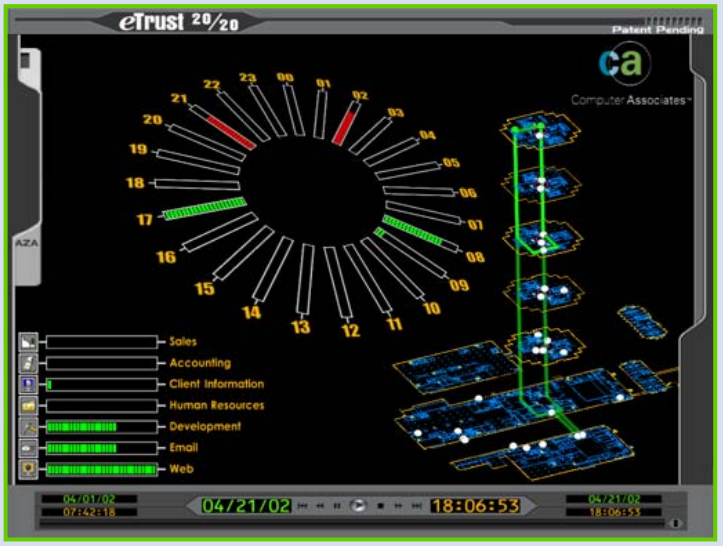
- **Vertrauenswürdigkeit der Beteiligten**
  - Instanzen für die Identifikation, Authentifizierung, Autorisierung
  - Beteiligte Hard- und Software bzw. deren Hersteller und Betreiber
  - Verteil- und Prüfwege
  - Aufbewahrungs- und Anwendungsart
- **Interoperabilität**
  - Technisch: Formate, Syntaxen, Semantik
  - Organisatorisch: Zeiträume, Nutzungsregeln
  - Rechtlich: Anerkennung, Regulation, Streitfälle
- **Missbrauch**
  - Staatlich: Repression, „Rasterfahndung“
  - Geschäftlich: Missbräuchliche Auswertungen/Weitergabe
  - Kriminell: Identitätsvortäuschung, Erpressung

IT-SECURITY - Forum #2

Sicherheits-Management



Holistisches Identitäts-Mgmt



Ausblick

Welche Initiativen/Konzepte/Architekturen setzen sich durch?

Welche Lieferanten können entsprechende, interoperable Erweiterungen ihrer Produkte vornehmen und „weiche“ Übergänge durch entsprechende Integration ermöglichen?

Für welche Kunden-/Nutzerbasis ist ein solcher Dienst von Interesse, und zu welchem Preis? Auf welcher wirtschaftlichen Basis kann ein entsprechender Dienst erbracht werden?

Welche rechtlichen / regulatorischen Anforderungen gelten – insbesondere bei grenzüberschreitenden Anwendungen ?

Wie kann trotz wachsender Komplexität und Bedrohungen das Vertrauen der Anwender hergestellt werden?