

Identity Management: Die 10 Top-Trends 2005

Martin Kuppinger
Kuppinger Cole + Partner
Digital ID Analysis + Evaluation
<http://www.kuppingercole.de>
mk@kuppingercole.de

Trends im Identity Management 2005

1. Federation
2. Compliance
3. Password Management
4. Phishing
5. RFID
6. Mobile Sicherheit
7. eGovernment und Privacy
8. Identity-basierende Anwendungen
9. Provisioning
10. Gesamtkonzepte für Access Management

Federation ist der Top-Trend im Identity Management 2005

- ❑ Federation: Gemeinsame, gesicherte Nutzung von Identitätsinformationen
- ❑ Unternehmensintern und unternehmensübergreifend
- ❑ Liberty etabliert sich als Standard, WS-* Standards werden noch brauchen und primär intern kommen
- ❑ 2005 gibt es die „awareness“ für Federation – die Projekte kommen danach
- ❑ Federation profitiert davon, dass es die Basis für die Lösung von konkreten Business-Anforderungen ist – klare Value Proposition

Compliance treibt die Investitionsentscheidungen

- ❑ In den USA schon heute das Top-Thema – hier fehlt noch der große Skandal
- ❑ Aber: Es gibt viele Compliance-Regeln - national, auf europäischer Ebene, international. SOX gilt ebenso wie HIPAA und andere US-Standards auch für viele europäische Unternehmen
- ❑ Getrieben wird das Thema derzeit nicht von der IT, sondern von Top-Management und Controlling
- ❑ Die IT muss aber die Basis dafür schaffen: **Wer** darf was machen? Und **wer** hat wann was gemacht? Es geht um digitale Identitäten.

Das Passwort ist tot – aber was kommt danach?

- ❑ Benutzername und Kennwörter (oder gar nur PINs) reichen für eine sichere Authentifizierung nicht mehr aus
- ❑ 2005 wird die Einsicht wachsen
- ❑ Die Lösungsanbieter werden aber 2005 noch kaum profitieren
- ❑ Hohe Kosten
- ❑ Akzeptanzhürden bei Nutzern (Biometrie) und IT – wer versteht schon wirklich PKIs?

Phishing: Die eigentliche Katastrophe steht noch bevor

- ❑ Phishing ist mittlerweile alltäglich...
- ❑ ...und wird zunehmend von Profis aus der organisierten Kriminalität statt Amateuren betrieben
- ❑ Riesiges Potenzial durch wenig informierte, unbedarfte Nutzer
- ❑ Erfolgreiches Phishing schlägt aber auf die zurück, auf deren Sites Nutzer zugreifen wollten: Banken und Online-Handel
- ❑ Dort wird versucht, das Problem auszusitzen – mit dem Hinweis auf die Verantwortung des Anwenders und die Kosten
- ❑ Verlorene Akzeptanz lässt sich aber nur unter hohen Kosten wieder herstellen

RFID kommt, ob wir wollen oder nicht

- ❑ RFID (Radio Frequency IDs) hat sinnvolle Einsatzszenarien vor allem in der Logistik und – mit Abstrichen – im Handel
- ❑ Die Technologie hat einen hohen Reifegrad, die Hürden liegen aber mehr und mehr in den Datenmengen
- ❑ 2005 wird das Jahr der großen Piloten und der konkreten Implementierungszeitpläne
- ❑ Wenn die Anbieter und Nutzer von RFID nicht aktive Aufklärung betreiben, droht aber eine Privacy-Diskussion, die nur schwer und mit hohen Kosten zu stoppen ist

Private PDAs werden 2005 in immer öfter verboten

- ❑ PDAs und Mobiltelefone haben immer größere Datenspeicher und immer mehr Funktionen
- ❑ Sie sind aber sicherheitstechnisch allenfalls auf dem Stand der ersten vernetzten PCs in den 80er Jahren – ein unkalkulierbares Sicherheitsrisiko
- ❑ Kaum zentrales Management, meist nur schwache Authentifizierung (wenn überhaupt), Kameras,...
- ❑ Nie war Datendiebstahl einfacher
- ❑ Unternehmen brauchen klare Regeln und Standards für die Nutzung privater PDAs und Mobiltelefone – Vereinheitlichung wird zum Thema
- ❑ Die Hersteller müssen darauf reagieren und ihre Systeme sicherer machen

Privacy muss neu definiert werden

- ❑ RFID, Gesundheitskarte, digitaler Personalausweis, Maut,...
- ❑ 2005 kommen viele Technologien mit konkreter Auswirkung auf Privacy
- ❑ Wer neue Technologien will, muss sie auch vermarkten – es braucht eine offene Diskussion über Datenschutz und die informationelle Selbstbestimmung, wenn sich diese nicht verselbständigen soll
- ❑ Erfolgreiches eGovernment setzt aufgeklärte Bürger, Ehrlichkeit und eine faire Kostenverteilung voraus

Firmen entdecken die Identität

- Application Security Infrastructures:
 - Definierte Regeln für die Sicherheitsinfrastruktur von eigenen und fremdentwickelten Anwendungen
 - Identitätsspeicher, Authentifizierung, Autorisierung
 - Keine Inseln mehr – statt dessen einheitliche Infrastrukturen
 - „Der Weg ist das Ziel“ – wenn 50% der neuen Anwendungen die Application Security Infrastructure nutzen, ist schon viel erreicht
- Identity-basierende Anwendungen
 - Musterbeispiel Client-Management
 - Die meisten Prozesse der Softwareverteilung sind identitätsbasierend (Neueinstellung, Jobwechsel, neues Projekt,...)
 - und müssen daher vom Identity Management-System ausgelöst werden

Provisioning – der Hype ist zu Ende

- ❑ Provisioning: Ein Bereich unter vielen im Identity Management – und immer noch einer der wichtigsten
- ❑ Das Marktwachstum wird anhalten
- ❑ Provisioning wird aber realistischer betrachtet als früher – es ist nicht die Lösung, die alles besser macht, sondern ein wichtiges Element und oft auch ein guter Einstieg in das Identity Management
- ❑ Das aber andere Infrastruktur-Elemente und Projektschritte (Datenbereinigung, Password Management,...) benötigt
- ❑ Und Provisioning ist nur ein Ansatz unter mehreren: Identitätsinformationen können unterschiedlich vereinheitlicht oder gemeinsam genutzt werden, vom gemeinsamen Verzeichnis über das Meta-Directory und Provisioning bis hin zu virtuellen Verzeichnissen und der Identity Federation
- ❑ Es gilt, den richtigen Ansatz für die jeweilige Problemstellung zu wählen

Die Firewall alleine bietet keinen ausreichenden Schutz mehr

- ❑ Es gibt nicht mehr nur einen oder wenige Stellen, an denen das Unternehmensnetzwerk geöffnet ist
- ❑ Immer mehr Prozesse laufen zwischen Kunden, Partnern und dem Unternehmen
- ❑ Es braucht ein Gesamtkonzept
 - Firewalls, die nicht nur die Frage beantworten, ob ein Paket durch darf oder nicht, sondern die Frage: „Welches Paket welcher digitalen Identität darf im Kontext welches Prozesses durch oder nicht durch?“
 - Access-Strategien für mobile Benutzer
 - Web Services Security bis auf die Content-Ebene
 - Spam-Filter im Kontext von digitalen Identitäten
 - ...