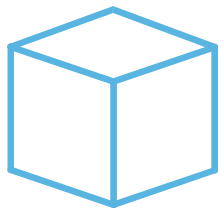
Základ bezpečnosti IT – jednotná správa používateľov

Radovan Semančík



BGS
Business Global Systems

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Záver

Súčasný stav IT Security

- Nekonzistentné bezpečnostné politiky
- Nekonzistentné databázy používateľov
- Perimeter security je neefektívna
- Rýchle vírusové infekcie
- Útoky z vnútra organizácie
- Patching doesn't work
- **Identity Crisis**

Identity Crisis

- Nikto nevie, kto má mať kam prístup
- Nikto nevie, kde všade má zamestnanec prístup
- Prístupy na firewall/VPDN iné ako do IS
- Mobility vs Security
- Vysoké náklady: help desk, prestoje, zmeny

It's clear identity has become a strategic business issue, not just a technology issue.

-- Jamie Lewis, president of consultancy Burton Group

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Záver

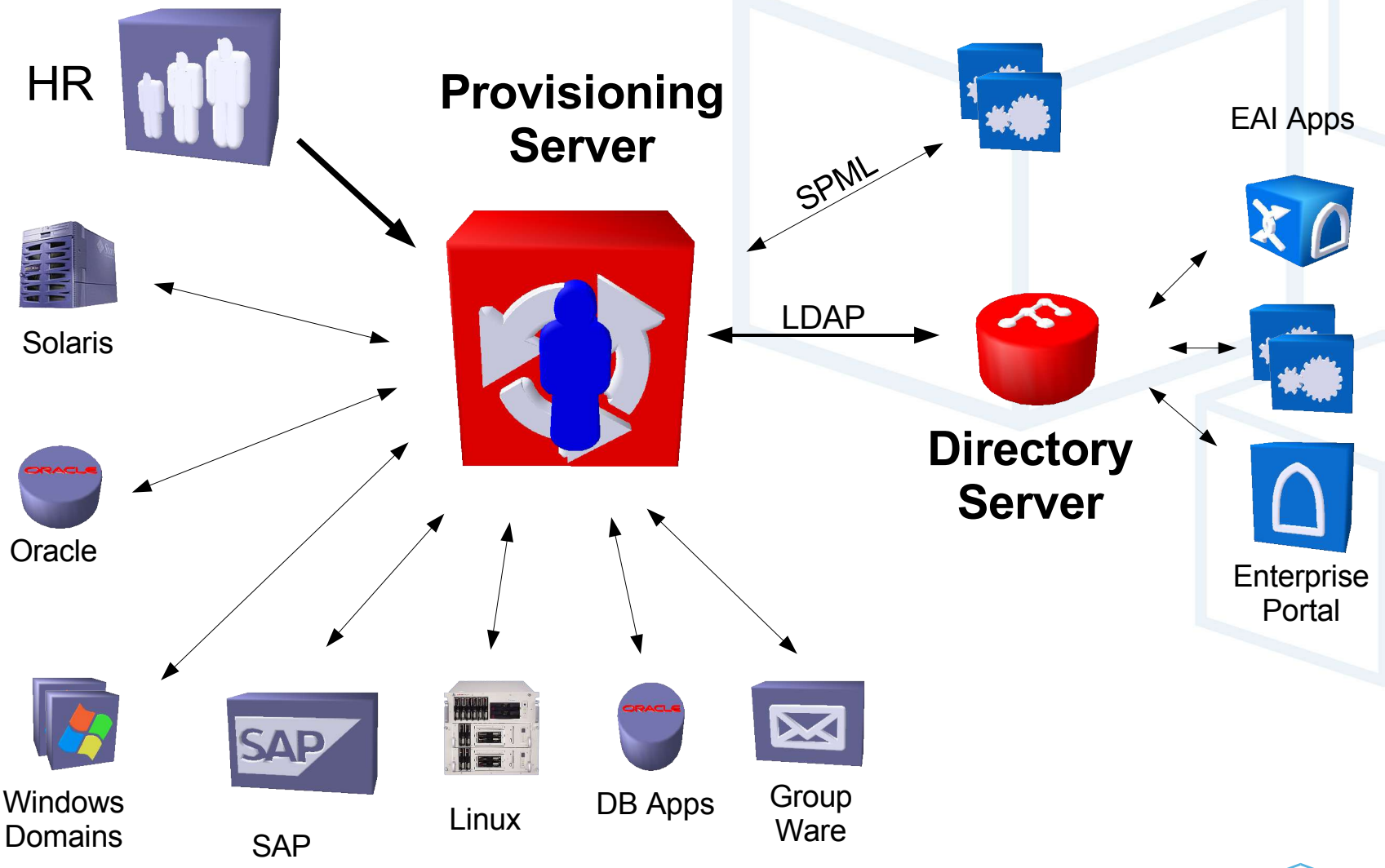
Mýtus centralizácie

- Jedna databáza/directory/repository
  - Nákladné na údržbu
  - Bezpečnostné riziko
  - Nie vždy technologicky možné (SQL join, offline, ...)
- Nutná synchronizácia
- Nekonzistencia
  - Rôzne UID
  - Rôzne typy prístupových práv
  - Neexistuje štruktúra rolí

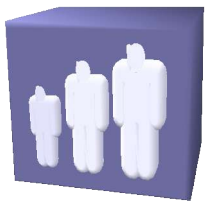
Technológie správy používateľov

- **Directory Server (LDAP)**
  - Nutná podmienka, nie však postačujúca
  - Len databáza, žiadna inteligencia
- **Provisioning system**
  - Synchronizácia údajov, workflow
  - Organizačná štruktúra role
- Metadirectory
  - Jednoduché pravidlá, obmedzenia (rovnaké uid)
- User Management, Doménové systémy, ...
  - Jednoduché, jednoúčelové, prvý krok

User Provisioning



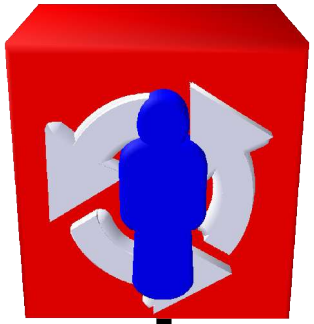
Spôsob práce Provisioning Servera



HR

34567889
Radovan
Semančík
IT Architect
System Division

Provisioning Server



LDAP

Directory Server

```
dn: uid=rsemancik,o=bgs
ou: sys
role: itArchitect
userPassword: ...
```

SSH

SQL

```
HR: 34567889
LDAP: uid=rsemancik,...
Solaris: semancik
Oracle: RSE
```

Solaris

```
semancik:x:101:100:Radovan Semancik:...
```

Oracle


```
RSE
Radovan Semancik
34567889
```


BGS Business Global Systems

Technologické rozdiely

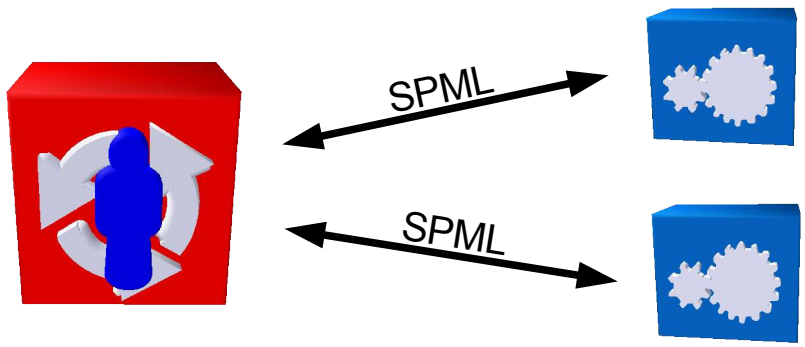
- Použitie Agentov
  - **Agentové technológie** („tesne viazané“, problematické)
  - **Bezagentové technológie** („voľne viazané“)
- Obsah centrálnej databázy
  - **Plné údaje** (zložitá synchronizácia, konzistenčné problémy)
  - **Len metadáta** (stála konzistencia, nižší výkon)
  - **Hybridné**
- Workflow
  - Rôzne úrovne flexibility

Dôležité špecifikácie

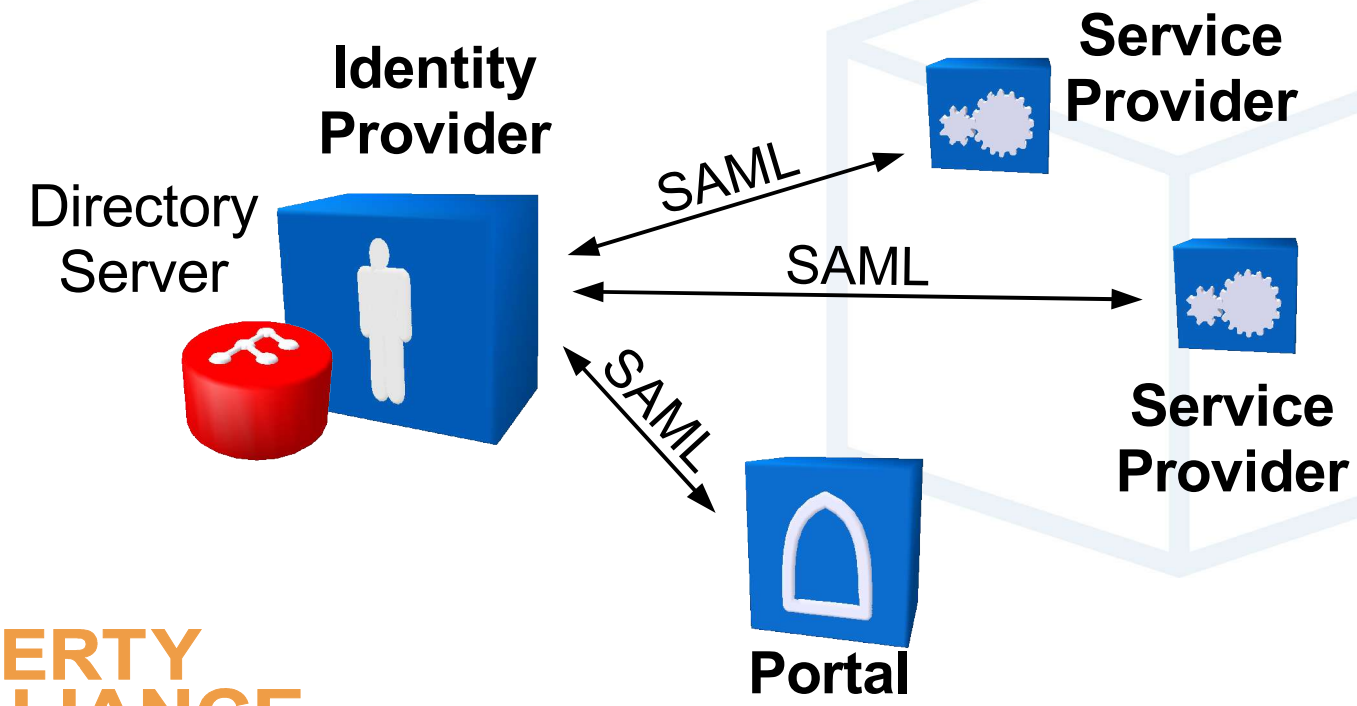
- Lightweight Directory Access Protocol (LDAP)
- Directory Services Markup Language (DSML)
- Service Provisioning Markup Language (SPML)
- Project Liberty Specification, Phase I
- Project Liberty Specification, Phase II
- WS-Security
- WS-Federation

Service Provisioning Markup Language

- Jazyk pre Provisioning systémy založený na XML
- Štandardizácia: OASIS Provisioning Services Technical Committee
- Založené na DSMLv2, spolupracuje so SAML a WS-Security
- Štandardné rozhranie – ľahká integrácia



Liberty Alliance Project



LIBERTY ALLIANCE

BGS Business Global Systems

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Záver

UUM vs PKI vs SSO

- **Unified User Management**
  - Jednotná správa používateľov
  - Nerieši autentifikáciu (len nepriamo)
- **Public Key Infrastructure**
  - Kryptografická infraštruktúra (nízkoúrovňová)
  - Nerieši správu používateľov (prístupové práva len okrajovo)
- **Single Sign On**
  - Autentifikačný systém
  - Nerieši správu používateľov
- **Digital Identity, Identity Management**

Záver

- Jednotná správa používateľov je prvý nutný krok
- PKI, Single Sign-On a Digital Identity až potom
- Orientácia na štandardy
- Dobrá architektúra, dobrý plán

> It is possible to deploy identity in incremental steps, but you won't succeed if you haven't built an overall plan before you start.
>
> -- Phil Becker, Digital ID World

Otázky

Ďakujem za pozornosť

Ing. Radovan Semančík

Business Global Systems, a.s.
Pluhová 2
83248 Bratislava

semancik@bgs.sk