SREČANJE *TECHNET ESS*

Srečanje TechNet – Enterprise Solutions Seminar je bilo organizirano 1. in 2. februarja 2006 v Portorožu in namenjeno strokovnjakom, ki delujejo na področju informacijske tehnologije (IT). Letos so bile predstavljene tehnološke novosti na področju 64-bitnih operacijskih sistemov, druga izdaja strežnika Windows 2003 Server R2, strežnik Windows Server "Longhorn", virtualizacija strežnikov in upravljanje z identitetami uporabnikov v heterogenih IT okoljih.

Upravljanje storitev IT – uvedba dobrih praks, Tomaž Čebul, Miro Budimir, Tomaž Šmid (Microsoft Slovenija)

Na predavanju je bil predstavljen ITIL (IT Infrastructure Library) kot okvir najboljše prakse in najpogosteje uporabljenih in sprejetih pristopov k upravljanju storitev IT. ITIL je tudi podlaga za standarda BS15000 in ISO/IEC 20000, ki urejata upravljanje teh storitev. Microsoftov MOF (Microsoft Operations Framework), ki je bil predstavljen pred približno tremi ali štirimi leti kot osnova priporočil za upravljanje storitev IT, se opira na vprašanje "s čim" in ne kot ITIL "kako".

In kakšen je današnji Microsoftov pogled na upravljanje storitev? Svetovni trendi kažejo padec stroškov, ki jih podjetja namenjajo za nakup opreme, hkrati pa je opazno naraščanje stroškov upravljanja in podpore. Trenutno razmerje stroškov je 30 odstotkov za novosti (implementacije) in 70 odstotkov za vzdrževanje storitev (za celotno IT). Stroški upravljanja rastejo zaradi kompleksnih in distribuiranih sistemov ter neorganiziranosti in pomanjkanja komunikacije. Problema se lotevajo tako, da:

- opredelijo in preučijo resnične potrebe organizacije,
- načrtujejo storitve, ki bodo ustrezale potrebam organizacije,
- uvajajo sisteme in procese, ki bodo zagotavljali te storitve in
- nepretrgoma spremljajo, nadzorujejo in izboljšujejo izvajanje storitev IT ter podpore znanju.

Da bi zadovoljili vse te zahteve, so potrebni sodobni in preverjeni pristopi. Eden teh je podpis pogodbe SLA (Service Level Agreement) med vodstvom podjetja in oddelkom IT: Pogodba določa pogoje za delovanje in vzdrževanje nekaterih servisov in se lahko podpiše za vsak servis posebej. Na seminarju je bil predstavljen primer pogodbe za upravljanje servisa, s katero se IT zaveže, da zagotovil namestitev, podporo in vzdrževanje servisa v omejenem času, običajno v enem letu. Vodstvo podjetja pa se zaveže, da bo v času izvajanja pogodbe zagotavljalo ustrezno izobraževanje za zaposlene v oddelku IT ter finančno podporo za vzdrževanje in nadgradnjo itd.

Za uvajanje upravljanja storitev in seznanjanje s to problematiko pred podpisom SLA je treba poznati:

- upravljanje zmogljivosti (angl. *performance management*),
- upravljanje sprememb in konfiguracij (angl. *change and configuration management*),
- načrtovanje simulacij in kapacitet (angl. *simulation/ capacity planning*).

Microsoft ima orodja za upravljanje:

- operations manager,
- system management server,
- system center capacity manager.

Vse skupaj naj bi povezoval System Definition Model (SDM), ki je del Visual Studio 2005 in zajema celostni pogled na aplikacije, storitve in sistem. O upravljanju razmišljamo že med razvojem, tako so relacije in predvidevanja že predstavljena, zahteve storitev pa so vgrajene že v fazi razvoja.

Želja vseh organizacij je, da za upravljanje storitev IT uporabijo izkušnje drugih podobnih organizacij ter ne odkrivajo že odkritega in ne ponavljajo napak, ki so jih storili drugi.

Prednosti 64-bitnih strežnikov, Boštjan Kosi (HP Slovenija)

HP je predstavil predvsem svoje proizvode, izdelane na osnovi 64-bitne tehnologije. Svoje proizvodne programe strežniških sistemov je skrčil s pet na dva. Sedaj jih pred-

stavljajo sistemi na osnovi procesorjev Itanium in sistemi na osnovi procesorjev x86 (Pentium, Xeon).

V seriji, ki temelji na Itaniumu, najdemo skupino sistemov HP NonStop in skupino sistemov HP Integrity. Že dobro znana serija strežnikov HP ProLiant temelji na procesorjih x86. S tem se je HP rešil starega bremena serije 9000 in Digitalovih sistemov Alpha. Konec proizvodnje strežnikov Alpha je predviden v septembru 2006.

Ta združitev v dve seriji prinaša HP-ju manjše stroške in večjo standardizacijo. To pa naj bi pomagalo zmanjšati tudi stroške končnemu uporabniku. Predstavljene so bile serije strežnikov po namembnosti in zgradbi. Sistemi Integrity Superdome so v bistvu večprocesorski sistemi, ki omogočajo strojno razdelitev (particioniranje). Na njih lahko hkrati tečejo različni operacijski sistemi, sistemski viri (resursi) pa se lahko dodeljujejo dinamično glede na potrebe. Zadnja skupina so t. i. sistemi Entry ali Access; predstavljeni so bili Proliant DL/ML (serije 300) in Blade, e-Class. Sistemi na osnovi Itaniuma, ki spadajo v to skupino, so RX (serije 2000, 4000 in 5000) in so namenjeni vstopnim storitvam za omrežja in spletne strežnike.

Predstavljena je bila arhitektura 64-bitne tehnologije v procesorjih Itanium 2, narejena s procesorji AMD 64. Pomembna lastnost procesorjev Itanium 2 je IA-32 Execution Layer, ki je v bistvu soprocesor za izvajanje 32-bitnih aplikacij. Zaradi tega je s temi procesorji možno zaganjati podedovane programe s posebnim "motorjem" (angl. *engine*) v sistemih Windows, ki je brezplačno na voljo na straneh MS.

Prednosti 64-bitnih procesorjev Itanium 2 se kažejo v možnosti izvajanja štirih ukazov (inštrukcij) v enem urinem ciklu, v arhitekturi notranjosti procesorja in različnih izvedbah predpomnilnika. Vse to daje tem procesorjem vodilno vlogo pri vgradnji v zmogljive sisteme. Velika zmogljivost je opazna predvsem pri obdelavi podatkov, saj SQL2005 deluje za 50 odstotkov hitreje kot na 32-bitnih sistemih.

Glede na vse prednosti, opisane na predavanju, in na strategijo razvoja 64-bitne tehnologije, je pametno že sedaj razmišljati o uvedbi takšnih strežnikov.

Kriza digitalne identitete v heterogenem okolju, Rafal Lukawiecki (Project Botticelli)

V uvodnem predavanju je Rafal Lukawiecki predstavil problematiko identitete v današnjem okolju IT. V bistvu se ta problem ne navezuje samo na poslovne procese, ampak na splošno uporabo informacijskih tehnologij na delovnem mestu, doma, v šoli in pri uporabi javnih servisov. Univerzalna identiteta trenutno še ni mogoča. Ker je bil internet zgrajen za anonimni dostop in ker lokalna omrežja uporabljajo različne, med seboj nezdružljive identitete, uporabniki v zadnjem času ne morejo več upravljati z vsemi svojimi identitetami. To pa nekateri s pridom izkoriščajo v kriminalne namene.

Pred letom 1980 je imel uporabnik običajno eno identiteto ali pa morda dve na centralnem strežniku. S prihodom aplikacij odjemalec/strežnik sredi osemdesetih so identitete uporabnika začele drastično naraščati. Današnja praksa kaže na problem identitet enega uporabnika za dostop do različnih servisov na spletu, dostop preko mobilnih naprav, pri prijavah v različne aplikacije na delovnem mestu ali na javnih servisih, v domačem omrežju ipd.

Kako so se problemi reševali? Vsak servis ali aplikacija ima mehanizem za overjanje (avtentikacijo), avtorizacijo in identifikacijske podatke za dostop do ponujenega servisa. Združevanje identitet uporabnika se je reševalo preko centralnega imenika, v katerem je bilo treba urediti povezave v sistemu za avtentikacijo med posameznimi servisi in dostopom uporabnikov do teh servisov. Zaradi vse večjega števila uporabnikov in servisov ter povezovanja med servisi se že pojavljajo težave z upravljanjem identitet. Glavni problemi so: preveč uporabnikov in preveč zahtev za administrativne pravice, preveč gesel, predolgi časi za prijavo (zaradi avtentikacije), preveč "sirot" – neuporabljenih ali pozabljenih identitet, omejeno upravljanje.

Iz tega sledi, da:

- povprečni uporabnik porabi na dan 16 minut za prijave,
- ima tipični uporabnik 12–18 identitet,
- se je število strani s potrebno registracijo samo v zadnjem letu povečalo za 1600 odstotkov,
- IT-operator v povprečju upravlja s 73 aplikacijami in 46 dobavitelji,
- postajajo zahteve glede pritožb in sledenja vse strožje,
- "osirotele identitete" predstavljajo velik varnostni problem.

Za reševanje tega problema obstajata dve rešitvi:

- zgraditev globalnega, vsestranskega in skupnega metasistema identitet, kar s časovnega vidika pomeni leto dni dela (boljša rešitev),
- zgraditev skupnega metasistema identitet na osnovi standardov za vse, ki bi uporabljali enake standarde (hitrejša rešitev).

Karakteristike metasistema identitet:

- ni sistem ali proizvod,
- je dogovor o metapodatkih in protokolih ter omogoča

več ponudnikov identitete,
- temelji na odprtih standardih,
- podpirajo ga vse tehnologije,
- vključuje zavedanje o zakonih, ki veljajo v okviru "identitete",
- spoštuje zasebnost.

Vzemimo za primer Microsoftov Passport: pokazalo se je, da je kot metasistem identitete neprimeren. Vendar pa je MS Passport ponudnik identitet za MSN, ki vsebuje več kakor 250 milijonov uporabnikov in preko njega se izvede na dan več kakor ena milijarda prijav. To pomeni, da je učinkovit. Če uporabimo Passport za javni dostop do interneta, se takoj opazi težava zaradi nezaupanja do tretjih uporabnikov, sistem ni več dovolj standarden, pojavijo se problemi z upravljanjem identitet (Ali dovoliti dostop do sistema za upravljanje identitet?). Največji problem pa je predelava aplikacij, da bi sploh lahko uporabljale takšen sistem.

MS Passport ne zagotavlja ideje o metasistemu identitet v najmanj dveh zgoraj omenjenih točkah.

Vloge v metasistemu identitet:

- Ponudniki identitete: pooblaščene organizacije, vladne organizacije ali morda tudi končni uporabniki, ki bi dajali zahtevke za identiteto (ime, starost, naslov itd.)
- Zaupanja vredni partnerji, ki bi ponujali vstopne točke, online servise itd.
- Stranke (individualne osebe) ali pravni subjekti, ki bi potrebovali identiteto.

Katera koli stranka v eni od vlog v metasistemu bi morala biti seznanjena z nadzorom identitete, minimalnim razkritjem identitete in omejeno uporabo ter opravičljivostjo uporabe v različne namene. Posest identitet ne bi smela predstavljati tveganja za razkritje uporabnikov, zato bi morali uporabniki imeti nadzor nad pretokom informacij o njihovih identitetah.

Predlagane rešitve naj bi zadovoljevale potrebe znotraj podjetja, spremembe pa naj bi bile potrebne šele po petih ali sedmih letih. V praksi, kjer so običajno potrebne takojšnje rešitve, bo potreba po upravljanju identitet za daljše obdobje izpolnjena z upoštevanjem karakteristik metasistema identitet.

V nadaljevanju je bil predstavljen Microsoftov sistem za upravljanje identitet (MS Identity Management System). To je skupek orodij, standardov in rešitev, ki zajema:

- Directory Services (Active Directory, ADAM, Extended Directory Services, PKI/CA, Services for Unix/ Netware),
- Access Management (AD Federation Services, Authorization Manager; Ent. Single Sign On, ISA Server),
- Identity Lifecycle Management (Identity Integration Server, BizTalk, Audit Collection Services, SQL Server Reporting).

Microsoft je že pripravil rešitve po standardih in priporočilih.

Upravljanje digitalne identitete, Rafal Lukawiecki (Project Botticelli)

Predavanje o funkcionalnosti proizvoda Microsoft Identity Integration Server (MIIS) se je navezovalo na prvi sklop predavanj o problemih digitalne identitete. Predstavljeni so bili enostavnejši dizajn, integriranje v že obstoječi sistem in upravljanje metapodatkov. Zadeva je uporabna predvsem v primeru, ko imamo več sistemov avtorizacije in avtentikacije. MIIS naj bi olajšal upravljanje uporabnikov v takih mešanih okoljih. Identiteti je na enostaven način mogoče sinhronizirati med različnimi sistemi. Vsebuje tudi sistem upravljanja z gesli (angl. *password management)*, ki je prijazen za uporabnika in ne potrebuje administratorja.

Alternativni načini avtentikacije, Rafal Lukawiecki (Project Botticelli)

Tretji del sklopa predavanj o krizi digitalnih identitet je opisoval pristop k močnejši avtentikaciji na osnovi Public Key Infrastructure (PKI), pametnih kartic (SmartCard), žetonov (Tokens), One Time Password (OTP) in SecureID ter uporabo biometričnih metod za avtentikacijo. Predstavljene so bile prednosti in slabosti teh tehnologij.

- **PKI**

  To je infrastruktura za praktično uporabo kriptografskih mehanizmov za avtentikacijo in avtorizacijo. Sama tehnologija je precej stara in preizkušena, vendar je preveč kompleksna za tipične uporabnike. Temelji na uporabi certifikatov in protokolov, ki zagotavljajo najvišjo verodostojnost pri avtentikaciji. Pri tej tehnologiji se med strankama ne prenašajo "skrivnosti", pa tudi noben neuporabljen podatek se ne zavrže. Možnosti, da bi kdo prisluškoval, skoraj ni. Za zaščito certifikata lahko uporabljamo posebno napravo (angl. token) ali geslo.

- **SmartCard**

  To so posebne fizične naprave, ki ščitijo privatni kriptografski ključ (podpis) pred nepooblaščenimi uporabniki. Ključ je zaščiten s posebno avtentikacijo. Naprava SmartCard v nobenem primeru ne sme razkriti privatnega ključa.

Običajno to niso kartice, temveč imajo obliko ključa USB, naprave Bluetooth, aktivne radiofrekvenčne identifikacije (RFID) ali integriranega čipa na kakšni napravi.

Vsaka resna naprava SmartCard mora zahtevati dodatno avtentikacijo z osebno identifikacijsko/izkazno številko (PIN), biometrično metodo. V nobenem primeru ne sme izdati informacije, ki jo nosi. To pomeni, da SmartCard vsebuje mehanizem, ki je združljiv z napravo, na kateri jo uporabljamo za preverjanje istovetnosti podatkov.

- **OTP (One Time Password) in SecureID**

  OTP je običajno kartica, ki na podlagi PIN-a generira neko vrednost – običajno geslo za sistem, na katerega se prijavljamo. Zaupanje med to kartico in sistemom pogojuje strojna oprema. Najbolj znan sistem OTP je SecureID.

- **Biometrika**

  Biometrika zajema identifikacijo (namesto avtentikacije) na podlagi fizičnih karakteristik osebe, in sicer:

  - slika (obraz, šarenica, očesna mrežnica, roke, papilarni vzorec),
  - zvok (govor, korakanje),
  - karakteristike pisave, obrazna mimika ipd.,
  - kemične lastnosti (ustni zadah, telesni vonj, zgradba lasu, tudi analiza DNA),
  - fiziologija (utrip, krvni tlak, temperatura, koncentracija kisika v krvi, pritiska v očesu).

  Ta tehnologija žal še ni tako dodelana, da na skenerju ne bi bilo mogoče ponarediti katere od zgoraj opisanih lastnosti. Priporočila za uporabo biometrike zajemajo predvsem nadzorovano okolje za identifikacijo in uporabo dodatnih metod avtentikacije, npr. s pametno kartico ali kako drugače.

  Prednost biometrike je enostavnost in uporabnost v kar nekaj okoljih. Neprimerna pa je za dnevne avtentikacije, ker ni mogoče zagotoviti, da je oseba, ki se identificira, res prava. Poleg tega je biometrične podatke možno z lahkoto ukrasti (lasje na oblačilih, prstni odtisi na vratih ...).

Pri večini načinov avtentikacije, predvsem pa pri uporabi biometrike, je pomembno pravilno nadzorovano okolje, v katerem se izvaja avtentikacija (identifikacija). Če se odločimo za biometrične metode, se moramo tudi zavedati kakovosti ali zanesljivosti skenerja ali senzorja.

Kaj pomeni kontrolirano ali nadzorovano okolje? Ob skenerju ali napravi, s katero se identificiramo, moramo imeti pričo, ki lahko zagotovi, da je bil na primer na skener nastavljen prst in ne kopija prstnega odtisa, da je pred kamero bilo oko in ne slika očesa ipd.

Avtentikaciji in posledično tudi avtorizaciji se ne moremo izogniti. Trenutne tehnologije se dopolnjujejo, razvijajo se novi načini avtorizacije. Tehnologija postaja vse bolj napredna, preizkušena in zanesljiva. V prihodnosti nas torej čaka enostavnejše upravljanje identitet, tako da bo imel vsak uporabnik le eno identiteto, s katero se bo lahko identificiral, storitve pa bodo vključevale akreditirane sisteme za izvajanje avtentikacije uporabnikov in upravljanje identitet.

Načini avtentikacij bodo verjetno večnivojski, potreben bo npr. prstni odtis ali slika šarenice, morda tu in tam še kakšna kartica SecureID. Zato pazite na svoje prste, oči, lase ...

Učinkovita izgradnja testnih okolij, Aleš Moškon (Microsoft Slovenija)

Predstavljena je bila migracija Microsoftovega testnega okolja na virtualno okolje. Tri tedne so porabili za namestitev 90 fizičnih strežnikov, s prehodom na virtualno okolje pa so prenesli funkcije s teh 90 strežnikov na 32 virtualnih strežnikov. Slednji se zaganjajo na devetih fizičnih strežnikih dva tedna. Za namestitev strežnika na fizični strežnik, namestitev strežnika *Virtual Server 2005* in preselitev funkcij na 32 virtualnih strežnikov so porabili tri ure. Seveda so imeli vnaprej pripravljene slike virtualnih strežnikov oziroma so jih prenesli s fizičnih strežnikov.

To prikazuje izredno dinamiko možnih sprememb, veliko nadgradljivost in predvsem zmanjšanje stroškov testnega okolja.

Kot virtualna infrastruktura tem testnim sistemom je bil predstavljen strežnik *Virtual Server 2005 R2*. Čeprav še ni verzije za Itanium, pa že normalno deluje na sistemih x68 s funkcijo EM.

Srečko Benčec