

Avtomatizacija IT - upravljanje uporabniških identitet

Marko Praprotnik, vodja oddelka za upravljanje, nadzor in varnost informacijskih sistemov.

Objavljeno v Varnostni forum, februar 2006

Varnost informacijskega sistema je pereč problem sodobnih organizacij. Največjo grožnjo informacijskemu sistemu predstavljajo notranji uporabniki. Po neodvisnih raziskavah so za največ varnostnih težav krivi prav zaposleni v organizaciji, pri čemer več kot polovico teh groženj predstavljajo uporabniki, ki škode ne povzročijo namenoma.

Izdelane varnostne politike in procedure za njeno izvajanje močno zmanjšujejo tovrstna tveganja, vendar ne predvidevajo možnosti napak uporabnikov ali upraviteljev. Upravljanje varnostnih elementov in pregledovanje njihovih dogodkov nam sicer omogoča kontrolo nad uspešnostjo varnostnih mehanizmov in odkrivanje napak, vendar se kljub temu velikokrat zgodi, da morebitna varnostna luknja postane predmet zlorab ali uporabniških napak.

Pomemben faktor upravljanja in implementacije varnostnih procedur, ki zmanjšuje možnosti upraviteljskih napak je uporaba avtomatizacije in programske verifikacije. Dober primer je upravljanje uporabniških identitet in njihovih dostopnih pravic, saj so ti postopki še vedno večinoma izdelani ročno oziroma le delno avtomatizirani.

Predvsem večje organizacije nenehno povečujejo število zaposlenih, partnerjev in dobaviteljev, ki lahko dostopajo do različnih informacijskih virov (operacijski sistemi, aplikacije ali podatkovne zbirke). Dostop do informacijskih virov je navadno zaščiten, zato morajo uporabniki pred vstopom identificirati (avtentikacija). Uporabniki lahko dokažejo svojo pristnost na podlagi identitete, ki jo pred tem vnesemo v ciljni informacijski vir in ji določimo ustrezne vloge. V primeru različnih informacijskih virov moramo poskrbeti, da imajo uporabniki dostop do samo upravičenih virov. Danes komunikacija o uporabnikih, ki potrebujejo dostop do določenih informacijskih virov, večinoma poteka preko elektronske pošte ali papirnega naloga. Tak način komunikacije in dodeljevanja oziroma odstranjevanja uporabniških pravic zahteva veliko časa. Izdelava uporabniških dostopov je velikokrat zelo zahtevna in zahteva dobro poznavanje ciljne tehnologije. Zato le-te lahko izdelajo le ustrezno usposobljeni upravitelji. To vsekakor vpliva na čas in stroške, ki so potrebni, da nov uporabnik lahko prične z nemotenim delom v organizaciji. Taki postopki so izpostavljeni človeškim napakam, zaradi katerih lahko pride do napačne dodelitve dostopnih pravic. Velik izziv je prav tako ažurno odstranjevanje nepotrebnih identitet in izdelava različnih analiz ter statistik.

Programska oprema za upravljanje identitet uporabnikov poskrbi za enostavno in avtomatizirano upravljanje in spremljanje življenjskega cikla identitet v mešanih oziroma heterogenih informacijskih okoljih. Programska oprema se odvisno od proizvajalca sestoji iz različnih sklopov, ki skupaj tvorijo funkcionalno celoto in se kot taki lahko dopolnjujejo. Prvi sklop je sestavljen iz uporabniškega imenika (Directory), v katerem so zapisani uporabniki, njihove lastnosti in pripadajoče uporabniške

identitete. Drugi sklop omogoča replikacijo in sinhronizacijo različnih uporabniških imenikov, tudi lastno razvitih. Tretji sklop omogoča upravljanje uporabniških identitet, njihovo izdelavo, odstranjevanje, spreminjanje, samopomoč uporabnikom, izdelavo analiz in statistik ter izdelavo in uveljavljanje različnih varnostnih politik in izdelavo različnih delovnih procesov (Workflow). Ostali sklopi skrbijo za enostavno avtentikacijo in avtorizacijo uporabnikov, beleženje aktivnosti ter vzpostavitev zaupanja in enotne avtentikacije med organizacijami (Federated Identity Management).

V grobem poznamo dva različna pristopa k upravljanju uporabniških identitet. Prvi je enostavnejši in izhaja iz potrebe po enotnem sistemu za upravljanje celotnega življenjskega cikla identitet, sinhronizaciji z različnimi uporabniškimi imeniki in možnostih izdelave statistik ter analiz. Pri tem pristopu je poudarek na samozahtevi in samopomoči uporabnikov. Uporabnik lahko na enostaven način zahteva dostop do določenega informacijskega vira in upravlja s svojimi uporabniškimi dostopi. Z njegovimi dostopi lahko upravlja tudi skrbnik informacijskega vira, njegov nadrejeni in podporna služba. Tak pristop se imenuje »Request Based Provisioning«. Drugi poleg funkcij prvega omogoča še upravljanje uporabniških identitet glede na vlogo uporabnikov. Uporabnikom so dostopi dodeljeni na podlagi njihove organizacijske pripadnosti. Z možnostjo sinhronizacije organizacijske strukture tako lahko poskrbimo za popolnoma samodejno izdelavo uporabniških identitet in dodelitev ustreznih dostopnih pravic na ustreznih virih. V primeru sprememb v organizacijski strukturi se lahko dostopne pravice uporabnikov dinamično spreminjajo. Tak pristop se imenuje »Role Based Provisioning«.

Pri obeh pristopih se lahko zahteva za dodelitev, odstranitev, spremembo uporabniške identitete izdelava v elektronski obliki in posreduje odgovornemu, ki s pritiskom na gumb sproži popolnoma avtomatiziran postopek takojšnje dodelitve ali odvzema pravic dostopa do vseh informacijskih virov, ki jih organizacija uporablja. Poslovnim procesom lahko popolnoma prilagodimo tok odobritve in število tistih, ki jih lahko odobrijo. V vsakem trenutku lahko izdelamo natančen spisek uporabnikov, ki lahko dostopajo do določenih informacijskih virov. V primeru sprememb dostopnih pravic neposredno na virih, s strani upraviteljev, lahko le-te zaznamo in jih glede na varnostno politiko tudi hitro ustrezno posodobimo, odstranimo ali o tem obvestimo odgovorne. Prav tako se na centralnem mestu lahko določa varnostna politika uporabniških imen in gesel, ki vključuje dolžino, kompleksnost, časovna okna, veljavnost in podobno.

Takšna programska oprema lahko z vmesnikom za končne uporabnike močno zmanjša obremenitev podporne službe, saj omogoča ponastavitev uporabniških gesel ter izdelavo zahtev za pridobitev drugih dostopnih pravic. S tako rešitvijo lahko omogočimo našim uporabnikom uporabo enotnih uporabniških imen in gesel na vseh virih. Ponastavitev gesel se lahko izvede na vseh virih hkrati in jo je mogoče izvesti direktno iz uporabniškega operacijskega sistema. V primeru izgube gesla lahko uporabnik s pomočjo pravih odgovorov na vprašanja popolnoma avtomatizirano zahteva ponastavitev vseh gesel na vseh virih, ki jih lahko uporablja ali pa to za njega stori podporna služba.

Zadnje čase posebno pozornost posvečamo vzpostavitvi medsebojnega zaupanja identitet med organizacijami. Sposobnost elektronskega poslovanja z dobavitelji, partnerji in kupci je dandanes ključnega pomena za uspešnost organizacij. Upravljanje tretjih identitet je navadno ročno, zamudno in drago. S pomočjo

ustrezne programske opreme lahko skrb za izdelavo uporabnikov, upravljanje, varnostno politiko in stroške podporne službe v celoti prepustimo našim zunanjim partnerjem. Namesto replikacije in sinhronizacije uporabniških identitet med različnimi uporabniškimi imeniki, ki se nahajajo v različnih organizacijah, lahko omogočimo dostop do virov na podlagi medsebojnega zaupanja. Z upravljanjem uporabniških identitet in dostopi do informacijskih virov, ki jih uporabljajo različne organizacije ali uporabniki se ukvarja »Federated Identity Management«. Vzpostavitev medsebojnega zaupanja urejajo standardi in specifikacije Liberty, SAML, WS-Federation, WS-Security and WS-Trust, ki jih mora programska oprema podpirati.

Ko smo ustrezno poskrbeli za to, da ima vsak od uporabnikov dostop do samo upravičenih informacijskih virov, je na vrsti ustrezna avtentikacija in avtorizacija uporabnikov. Le-to lahko izvajamo z različnim orodji, ki so del zgoraj navedenih rešitev in skrbijo za dostop uporabnikov do operacijskih sistemov, raznih lastno in ne-lastno razvitih aplikacij, spletnih strežnikov in podobno. Za avtentikacijo uporabnikov lahko uporabimo različne varnostne mehanizme, ki ugotovljeno identiteto uporabnika preverijo z avtorizacijskim mehanizmom in na podlagi tega dovolijo ustrezen dostop do informacij. Istočasno sistem poskrbi za natančno beleženje vseh aktivnosti, izdelovanje statistik in alarmiranje v primeru zlonamernih akcij.

Predstavljene rešitve za enostavno in centralizirano upravljanje uporabniških identitet skozi celotno življenjsko dobo in avtentikacijo ter avtorizacijo uporabnikov z možnostjo uporabe sistema enkratne prijave (single sign-on) znižujejo stroške organizacije in zagotavljajo večji nadzor, varnost ter razpoložljivost informacijskega sistema.

»Kot bi za stanovanje, pisarno, vikend in avto uporabljali isti ključ. To bi bilo enostavno, a nevarno. Če bi tak ključ lahko varno in enostavno izdelali in zamenjali na vseh lokacijah hkrati, bi bila to popolna rešitev.«