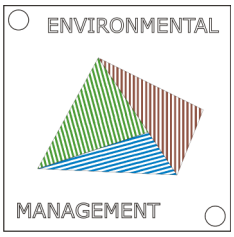
RUSKO, M. – BALOG, K. [Eds.] 2007:
Manažérstvo životného prostredia 2007 ▼▲▼ Management of Environment ´2007
zo VII. konferencie so zahraničnou účasťou konanej 5. - 6. 1. 2007 v Jaslovských Bohuniciach
Proceedings of the International Conference, Jaslovské Bohunice, 5-6 January 2007
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-18-3.



BEZPEČNOSTNÉ METÓDY PRE OCHRANU PRACOVNÝCH STANÍC ENVIRONMENTÁLNEHO INFORMAČNÉHO SYSTÉMU

PAVOL VOJTEK

SAFETY METODS FOR PROTECTION THE WORK STATIONS TO ENVIRONMENTAL INFORMATION SYSTEMS

ABSTRAKT
Témou príspevku je poukázať na možnosť využitia jednej z účinných metód, pomocou ktorej dosiahneme požadovanú úroveň bezpečnosti a ochrany pracovných staníc pre EIS. Práve pracovné stanice všeobecne predstavujú značné riziko neautorizovaného použitia zdrojov informačného systému. IS chránime pred jeho neoprávneným použitím neautorizovanými používateľmi, implementovaním podpory digitálnych certifikátov umiestnených na smart kartách.
Kľúčové slová: *overenie klienta, overenie servera, certifikačná autorita*

ABSTRACT
The topic of contribution is to point out the possibility of utilization one of the effective method, through it, we achieve required level for safety and protection the work stations to EIS. The work stations generally present large risk for non-authorised using the sources of information system. We protect IS against its illegitimate using with non-authorised users so that we implement the support of digital certificates that are placed on the smart cards.
Key words: *client authentification, server authentification, certification authority*

Úvod

Každá environmentálna organizácia, alebo firma v záujme kvalitného zabezpečenia svojich prvoradých funkcií musí prijať opatrenia smerujúce k primeranej ochrane svojich významných aktív. To platí aj pre prevádzkovateľa EIS. Je potrebné si uvedomiť, že najväčšie riziko napadnutia citlivých dát je práve z vnútorného prostredia (obvykle až 70%).

Dá sa konštatovať, že najväčším rizikom pre prevádzkovateľa IS je rozsiahly neautorizovaný únik citlivých údajov, ktorých prezradenie alebo zničenie by mohlo ohroziť funkčnosť prevádzkovateľa environmentálneho IS, alebo jeho dobré meno.

Zámerom tohto príspevku je poukázať práve možnosť využitia jednej z účinných metód, kde na základe princípu voliteľného riadenia prístupu, v ktorom prístupové práva určuje vlastník, dosiahneme požadovanú úroveň bezpečnosti a ochrany pracovných staníc pre EIS.

RUSKO, M. – BALOG, K. [Eds.] 2007:
Manažérstvo životného prostredia 2007 ▼▲▼ Management of Environment ´2007
zo VII. konferencie so zahraničnou účasťou konanej 5. - 6. 1. 2007 v Jaslovských Bohuniciach
Proceedings of the International Conference, Jaslovské Bohunice, 5-6 January 2007
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-18-3.

BEZPEČNOSTNÉ METÓDY PRE OCHRANU PRACOVNÝCH STANÍC EIS

Pri prístupe k zdroju údajov by sa mal používateľ identifikovať a autentifikovať. Preto je potrebné tieto zdroje údajov chrániť tak, aby sa dosiahli základné atribúty bezpečnosti v ktorejkoľvek časti environmentálneho IS. Operácie s údajmi na všetkých úrovniach musia byť zaznamenávané. Záznamy musíme vedieť analyzovať a vyhodnocovať. V prípade, že sa zistí narušenie bezpečnosti, musíme vedieť viesť vyšetrovanie s cieľom objasniť príčiny, pôvod incidentu, eliminovať jeho následky a vyvodiť dôsledky.

Bezpečnostná architektúra informačného systému musí spĺňať požiadavky na úrovni platných noriem, technologicky nezávislých štandardov a praktík, ktoré slúžia na dosiahnutie bezpečnostných požiadaviek stanovených bezpečnostnou politikou prevádzkovateľa environmentálneho IS.

V prípade ochrany pracovných staníc je potrebné chrániť IS pred jeho neoprávneným použitím neautorizovanými používateľmi, napríklad implementovaním podpory čipových kariet. Práve pracovné stanice všeobecne predstavujú značné riziko neautorizovaného použitia zdrojov informačného systému.

V rámci technického riešenia preto vychádzame z predpokladu, že v prístupovej úrovni pracovných staníc sa bude používať výhradne operačný systém MS Windows. Ochranu pracovných staníc rozšírime a doplníme o ďalší stupeň bezpečnosti. Pri prihlasovaní sa používateľov k pracovnej stanici, budeme vyžadovať čipovú kartu, ktorá bude obsahovať šifrovací (privátny) kľúč, jednoznačne identifikujúci vlastníka. Tento kľúč bude na karte chránený PIN kódom, ktorý pozná len jeho vlastník. Tým zabezpečíme väzbu používateľ – karta – účet v systéme a bude zabezpečená vysoká miera bezpečnosti. Par kľúčov generuje samotná karta - token a ten aj zabezpečuje ich ochranu. Aby bolo vylúčené falšovanie kľúčov, je použitý mechanizmus certifikácie ich verejných častí certifikačnou autoritou prevádzkovateľa EIS.

Certifikačná Autorita, ktorá pre svoju prevádzku vyžaduje služby technológie Active Directory, vydáva certifikáty na základe žiadostí zo siete, ktoré musia byť autentifikované v doméne, a vydáva ich okamžite. Doba ich platnosti je daná kľúčom v registroch a typom certifikátu. Hodnoty môžeme prednastaviť na 1, respektíve na 2 roky.

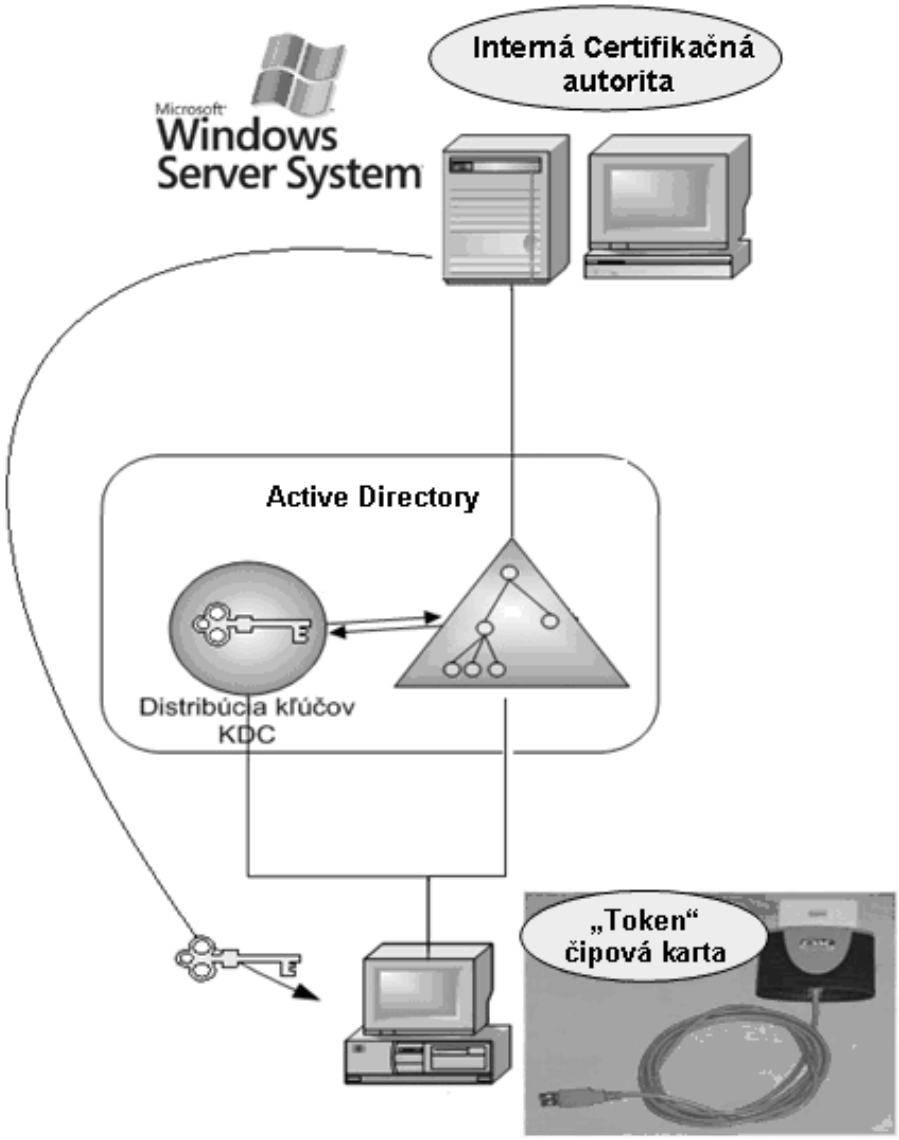
Použitie certifikátov vydávaných Windows 2003 Certifikačnou Autoritou je všeobecne možné na tieto účely:

- server authentication – overenie servera voči klientovi
- client authentication – overenie klienta voči serveru, napr. vzdialený prístup
- kombinovaný s overením používateľa pomocou čipovej karty
- code sign – podpisovanie programových balíkov, inštalácií, knižníc a pod.
- secure e-mail – zabezpečenie elektronickej pošty šifrovaním a podpisovaním správ
- EFS – šifrovanie súborov a adresárov na uložených na diskoch
- IPsec – šifrovanie sieťovej komunikácie v prípade prípravy aplikačného
- programového vybavenia overenie používateľa v aplikácii

V návrhu systémového riešenia ochrany pracovných staníc si zakladáme na požiadavke silnej identifikácie používateľa a riadeného prístupu používateľov k dátovým zdrojom EIS.

Keďže sme si zvolili OS MS Windows, je potrebné pristúpiť za účelom riadenia k systému doménovej štruktúry v súvislosti s presadzovaním bezpečnostnej politiky až na pracovné stanice. Operačný systém pre pracovné stanice, ktoré budú zaradené do domény je možné použiť z hľadiska bezpečnostného systému na ochranu pracovných staníc nasledovný:

- Microsoft Windows XP Professional
- Microsoft Windows Vista



Obr. Autentifikácia pomocou čipovej karty

Jednotlivý klienti sa budú prihlasovať na server cez internú sieť LAN. Klienti sa budú musieť povinne prihlasovať do domény pomocou čipovej karty. Bez tejto karty nebude mať užívateľ prístup k pracovnej stanici ani ku zdrojom domény. Na karte sú uložené bezpečnostné kľúče a certifikáty k jednotlivým kľúčom. Na základe týchto certifikátov a PIN kódu sa užívateľ prihlási automaticky do domény.

Systémový inžinieri budú mať možnosť spravovať svoj priestor v doméne a zároveň udržiavať aktuálnu organizačnú štruktúru v doméne. Bezpečnostné nastavenia pre jednotlivé pracovné stanice nastavuje a spravuje doménový správca. Iba správca bude mať k týmto nastaveniam prístup. Tým zaručíme distribúciu bezpečnostných nastavení na každú pracovnú stanicu zaradenú do doménovej štruktúry, respektíve každého užívateľa v doméne. Na prihlásenie užívateľa do pracovnej stanice sa bude vyžadovať čipová karta, na ktorej bude mať užívateľ uložené bezpečnostné kľúče a certifikát. Certifikačná autorita pre potreby domény bude v sieti LAN a bude začlenená do Active Directory.

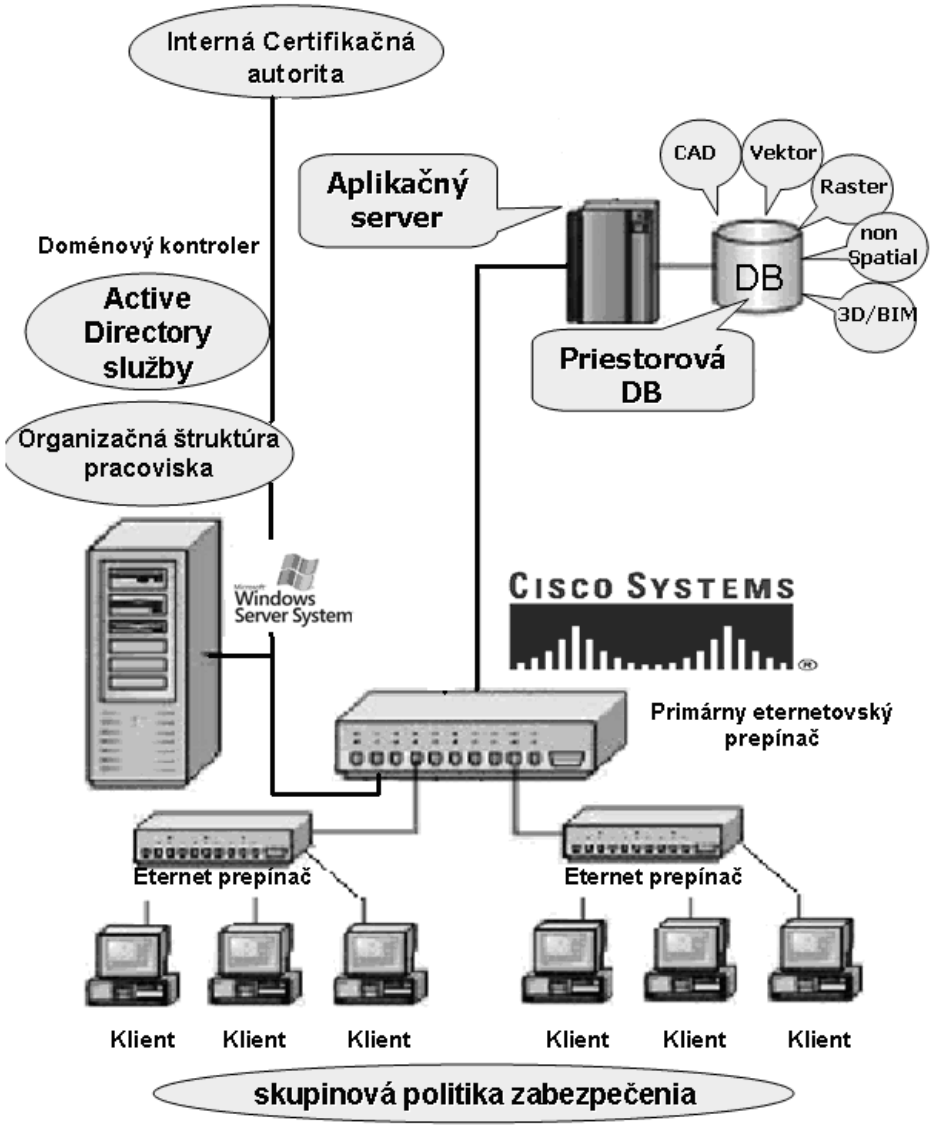
Politiku lokálnych pracovných staníc pri nasadení bezpečnostného systému na ochranu pracovných staníc nebudeme požívať, ale použijeme skupinovú politiku ktorá je nadradená politike lokálnej pracovnej stanice pri použití doménovej štruktúry.

Užívateľ sa pomocou čipovej karty prihlási automaticky do domény a tým sa na pracovnú stanicu respektíve užívateľa aplikuje skupinová politika pre danú organizačnú jednotku. Zároveň sa aplikujú aj skupinové politiky z nadradených organizačných jednotiek. Skupinové politiky sa dajú aplikovať na organizačné jednotky, alebo na celú doménu.

Bezpečnostná politika pre pracovné stanice bude aplikovaná na úrovni organizačných jednotiek pre lepšiu správu doménovej štruktúry. Pre použitie jednotného klienta bude vytvorená jedna skupinová politika a táto bude aplikovaná na jednotlivé organizačné jednotky. Pri akejkoľvek zmene tejto politiky budú zmeny automaticky platné pre všetky pracovné stanice respektíve autorizovaných užívateľov zaradených do týchto organizačných jednotiek. Tým sa zamedzí náhodným chybám pri vytváraní a aplikovaní samostatných skupinových politík pre každú organizačnú jednotku. Politika konta bude aplikovaná na úrovni celej domény, aby v doméne neexistovali autorizovaný užívatelia s ľahko dostupnými heslami.

Na základe praktických skúseností môžeme predpokladať aj situáciu, keď si autorizovaný užívateľ zabudne svoju čipovú kartu. V takýchto prípadoch je možné aby správca domény povolil užívateľovi prístup do domény prihlasovaním len pomocou mena a hesla (šifrovacie služby na ktoré je potrebný privátny kľúč nebudú dostupné). Toto riešenie bude len dočasné a sprostredkuje autorizovanému užívateľovi možnosť pracovať aj bez použitia čipovej karty v takýchto prípadoch.

Na nasledujúcom obrázku je uvedená IT architektúra pracoviska s koncovými pracovnými stanicami, s integrovaným doménovým serverom, ktorý slúži aj pre riadenie a správu používateľov a ich prístupových práv prostredníctvom technológie Activ directory. Začlenená je aj Certifikačná autorita (CA) pre poskytovanie a správu digitálnych certifikátov a nakoniec aplikačné a databázové servery pre environmentálne aplikácie.



Obr. Systémová architektúra aplikácie pre EIS

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] BOTT, E. – SIECHERT, C.: Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Praha, Computer Press, 2004, ISBN: 80-722-6878-3, 696 s.

[2] DOSEDĚL, T.: Počítačová bezpečnosť a ochrana dát. Praha, Computer Press 2004 ISBN 80-251-0106-1 ,200 s.

[3] CHOVANCOVÁ, J. - MAJERNÍK, M.: Environmentálny reporting ako nástroj vonkajšej komunikácie podniku. In: Trendy v systémoch riadenia podnikov : 9. medzinárodná vedecká konferencia, Herľany, 26.-27. október 2006 : Zborník príspevkov. Košice : TU, 2006. 6 s. ISBN 80-8073-660-X.

[4] CHOVANCOVÁ, J. - HERCZNER, P: Špecifikácia indikátorov pre účely environmentálneho reportingu. In: Novus scientia 2006 : 9. celoštátna konferencia doktorandov technických univerzít a vysokých škôl, 6.12.2006, Košice : Zborník referátov. Košice : TU-SjF, 2006. s. 189-194. ISBN 80-8073-354-6.

[5] RUSKO, M., 2004. Environmentálne orientovaný manažment v praxi manažéra. - Žilina: Strix [VeV]. Edícia EV-2, Prvé slovenské vydanie, ISBN 80-969257-1-7, 190 s.

[6] YEGULALP, S.: Microsoft Windows Server 2000/2003. Nedokumentovaná řešení. Brno, CP Books 2004, ISBN 8025101460, 296 s.

ADRESA AUTORA

Ing. Pavol Vojtek, Sociálna poisťovňa, pobočka Prešov, Slovenská republika**,** e-mail: >Pavol.Vojtek@hotmail.com<

RECENZENT

Doc. Ing. Jozef Halász, PhD., Technická Univerzita, Strojnícka fakulta, Katedra environmentalistiky a riadenia procesov, Park Komenského 5, 042 00 Košice, Slovenská republika