ATENŢIONARE!

Conţinutul acestei platforme de instruire a fost elaborat în cadrul proiectului „**Dezvoltarea resurselor umane în educaţie pentru administrarea reţelelor de calculatoare din şcolile româneşti prin dezvoltarea şi susţinerea de programe care să sprijine noi profesii în educaţie, în contextul procesului de reconversie a profesorilor şi atingerea masei critice de stabilizare a acestora în şcoli, precum şi orientarea lor către domenii cerute pe piaţa muncii**". Conţinutul platformei este destinat în exclusivitate pentru activităţi de instruire a membrilor grupului ţintă eligibil în proiect.

Utilizarea conţinutului în scopuri comerciale sau de către persoane neautorizate nu este permisă.

Copierea, totală sau parţială, a conţinutului de instruire al acestei platforme de către utilizatori autorizaţi este permisă numai cu indicarea sursei de preluare (platforma de instruire eadmin.cpi.ro).

Pentru orice probleme, nelămuriri, sugestii, informaţii legate de aspectele de mai sus vă rugăm să utilizaţi adresa de email: proiect.eadmin@cpi.ro

Acest material a fost elaborat de Mihaela Tudose, expert la S.C. Centrul de Pregătire în Informatică S.A., partener de implementare a proiectului POSDRU /3/1.3/S/5.

Versiunea materialului de instruire: V2.0

Securitatea reţelelor Microsoft

Concepte generale

Securitatea reţelelor de calculatore este un subiect destul de complicat dar foarte actual, în condiţiile în care, din ce în ce mai multe persoane au acces la calculatoare conectate în reţea şi la resursele distribuite în diferite reţele de calculatoare. Nu numai administratorii ci şi utilizatorii trebuie să fie interesaţi de securitatea reţelelor, să înţeleagă riscurile şi să aplice cele mai potrivite soluţii pentru asigurarea securităţii datelor şi a transmisiilor de date. Securitatea reţelelor şi a calculatoarelor care le compun se referă la datele păstrate, inclusiv mesajele e-mail, baze de date cu conţinut confidenţial, tranzacţii şi componente de tranzacţii de tipul e-*commerce.* Pentru că tot mai mulţi specialişti IT sunt preocupaţi de asigurarea securităţii reţelelor de calculatoare au apărut organizaţii specializate. SANS (http://www.sans.org) este lider în cercetarea, certificarea şi instruirea în domeniul securităţii informaţiei. Institutul SANS (*SysAdmin, Audit, Network, Security*) a fost înfiinţat în 1989 ca organizaţie de cercetare şi şcolarizare. El pune la dispoziţia celor interesaţi cunoştinţele şi experienţa profesioniştilor în securitate IT. Buletinele informative, rezumate ale studiilor şi cercetărilor, alerte de securitate identificate sunt informaţii gratuite şi sunt întotdeauna o sursă de inspiraţie pentru rezolvarea problemelor şi a incidentelor de securitate.

Evaluarea gradului de protecţie a unei reţele sau a unui calculator porneşte de la identificarea ameninţărilor şi a vulnerabilităţilor: ameninţările sunt pericole care pot influenţa buna funcţionare, iar vulnerabilităţile sunt punctele slabe prin care se pot exercita atacuri atât din interiorul cât şi din exteriorul reţelei. Cele mai comune ameninţări, care găsesc din păcate şi breşe de securitate, respectiv vulnerabilităţi prin care pot manifesta, sunt: furtul de date, furtul de coduri sursă ale aplicaţiilor aflate în dezvoltare, furtul de identitate prin folosirea informaţiilor şi a datelor cu caracter privat ca urmare a expunerii acestora într-un mod necontrolat, instalarea şi lansarea în execuţie a software-ului maliţios şi, nu în ultimul rând, dezastrele naturale.

Asigurarea securităţii foloseşte conceptul de management al riscurilor cu scopul de a găsi cele mai bune răspunsuri şi reacţii în faţa ameninţărilor cunoscute. Managementul riscurilor are la bază studiul atent al criteriilor şi condiţiilor de apariţie a riscurilor, impactul ameninţării asupra reţelei şi a calculatoarelor care o compun, valoarea estimată a pagubelor şi costurile implementării soluţiilor care pot asigura securitatea. În urma unei astfel de evaluări se poate decide care este răspunsul cel mai bun în faţa ameninţărilor şi care sunt cele mai bune reacţii la apariţia incidentelor de securitate.

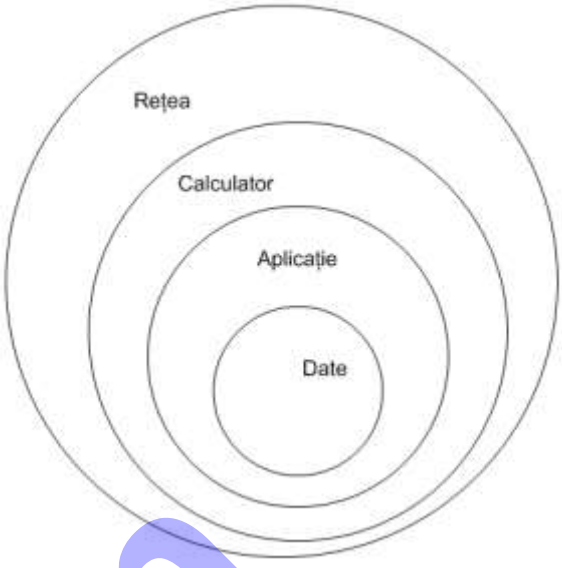
În domeniul reţelelor de calculatoare, securitatea se referă la adoptarea de către administratorul de reţea a celor mai potrivite strategii, care să protejeze reţeaua şi resursele accesibile prin reţea faţă de accesul neautorizat. În plus, administratorul de reţea va avea grijă să măsoare şi să monitorizeze periodic eficienţa – sau lipsa de eficienţă – a măsurilor implementate.

Un posibil scenariu de securitate a reţelelor începe cu autentificarea utilizatorilor, în mod normal prin folosirea unui cont de utilizator şi a unei parole. Parola este ceva ce utilizatorul „ştie, cunoaşte" şi se spune despre autentificarea de acest tip că este o autentificare cu un singur factor. Autentificarea prin doi factori foloseşte în plus ceva ce „are" utilizatorul, cum ar fi un jeton, un card, un telefon mobil. Autentificarea prin trei factori cuprinde şi ceva „ce este" utilizatorul: amprenta digitală sau palmară, imaginea scanată a retinei, amprenta vocală. O dată autentificat, ar trebui să intre în funcţiune procedurile şi politicile de acces prin care utilizatorul este autorizat să folosească numai anumite resurse şi servicii disponibile în reţea. Autentificarea şi autorizarea utilizatorilor nu sunt suficiente în faţa unui software maliţios trimis prin reţea, cum sunt viruşii, viermii, caii troieni. Protecţia antivirus şi sistemele de detecţie a intruziunilor ar putea fi o soluţie bună în acest caz. Ar mai fi nevoie de proceduri specializate pentru monitorizarea traficului de date în reţea, în căutarea traficului neaşteptat şi pentru identificarea comportamentului neobişnuit, chiar bizar, al unor servicii sau aplicaţii. Evenimentele trebuie jurnalizate şi analizate ulterior. Se întâmplă să fie nevoie câteodată de transmisii criptate de date între calculatoare din reţea, cu scopul de a asigura confidenţialitatea informaţiilor.

Securitatea reţelelor este o componentă a sistemului de securitate a informaţiei. Securitatea informaţiei se referă în general la protejarea informaţiei şi a sistemelor informatice faţă de accesul neautorizat, utilizarea, expunerea, modificarea şi distrugerea informaţiei. Securitatea are în vedere asigurarea confidenţialităţii, integrităţii şi a disponibilităţii informaţiei. Procedurile şi strategiile de securitate implementate au rolul de a specifica administratorilor şi utilizatorilor în general cum să folosească aplicaţiile şi echipamentele astfel încât să asigure securitatea informaţiei la nivelul organizaţiei.

Apărarea în profunzime şi managementul riscului

Informaţia trebuie protejată pe toată durata de viaţă, de la obţinere până la utilizarea ei finală, completă. Ea va fi protejată când se află în mişcare, la fel ca şi în varianta statică. Informaţia poate parcurge mai multe stadii de prelucrare şi va trebui să fie protejată şi în timpul prelucrării.



Robusteţea oricărui sistem este egală cu cea a verigii celei mai slabe. Folosind strategia apărării în profunzime, dacă o procedură de apărare nu este suficientă pentru a asigura protecţia datelor, atunci următoarea va putea oferi protecţia aşteptată.

În sens larg, procesul de management al riscului constă din:

1. identificarea şi estimarea valorii bunurilor care au legătură cu informaţia, cu păstrarea şi folosirea ei în siguranţă. Se includ aici: persoane, încăperi şi clădiri, componentele hardware, cele software, datele însele indiferent de forma în care sunt păstrate – format electronic, tipărituri, manuscrise.
2. evaluarea ameninţărilor: condiţii de forţă majoră identificabile, accidente, acte de rea voinţă care îşi au originea în interiorul sau în exteriorul organizaţiei.
3. evaluarea vulnerabilităţilor şi, pentru fiecare vulnerabilitate identificată, estimarea probabilităţii ca această vulnerabilitate să fie exploatată, folosită; va fi nevoie şi de identificarea şi evaluarea politicilor, procedurilor, standardelor care ar putea fi aplicate în calitate de contramăsuri asociate vulnerabilităţilor identificate.
4. calcularea impactului pe care îl are fiecare vulnerabilitate asupra bunurilor; va fi folosită analiza cantitativă şi calitativă.
5. identificarea, selectarea şi implementarea contramăsurilor potrivite: politici, proceduri de securitate.
6. evaluarea eficienţei aplicării politicilor şi procedurilor de securitate; aplicarea măsurilor de securitate nu ar trebui să afecteze productivitatea muncii şi nici desfăşurarea în bune condiţii a activităţilor curente ale organizaţiei.

Unele riscuri ar putea fi acceptate, pornind de la valoarea mică a bunurilor afectate de acel risc, de la frecvenţa mică de apariţie a unui anume risc şi de la impactul nesemnificativ asupra desfăşurării activităţilor organizaţiei. Altele pot fi diminuate, atenuate prin alegerea şi implementarea celor mai potrivite proceduri şi politici de securitate. În anumite situaţii riscurile pot fi transferate prin externalizarea unor operaţii şi activităţi sau prin asigurarea bunurilor implicate prin poliţe de asigurare.

Riscurile pot fi diminuate, atenuate prin implementarea procedurilor, politicilor, a măsurilor de securitate.

Nivelul măsurilor de securitate	Descriere
Administrativ	Controlul administrativ constă din documente scrise care conţin politicile, procedurile, standardele, ghidurile aprobate de către managementul organizaţiei. Ele formează cadrul în care se desfăşoară toate activităţile organizaţiei respective. Documentele informează asupra modului în care se desfăşoară activitatea curentă, asupra regulilor şi regulamentelor aflate în vigoare. În astfel de documente ar trebui să apară, de exemplu, regulile de folosire a parolelor, regulile de utilizare a echipamentelor şi a componentelor software, împreună cu eventualele sancţiuni aplicabile în situaţia nerespectării lor.
Software	Măsurilor aplicabile prin componente software sunt cele prin care poate fi monitorizat (supravegheat) şi controlat accesul utilizatorilor la informaţiile de orice fel şi la calculatoare. Controlul accesului poate fi implementat prin: parole, proceduri sau servicii de tip *firewall*, sisteme pentru detectarea intruziunilor în reţea, liste de tip ACL (*Access Control List* – vezi permisiuni la fişiere, foldere, obiecte *Active Directory*), proceduri pentru criptarea datelor şi a transmisiei de date, proceduri pentru securizarea documentelor (vezi – criptarea fişierelor). Măsuri de securitate importante sunt cele implementate ca efect al principiului „**privilegiul cel mai mic**”. Conform acestui principiu, oricărei persoane, program sau proces sistem nu i se vor acorda decât privilegiile minime, suficiente

	pentru rezolvarea sarcinilor. Un exemplu de abatere de la acest principiu este reprezentat de deschiderea de sesiune folosind un cont cu privilegii de administrare doar pentru citirea mesajelor *e-mail* şi navigarea prin Internet. Un alt exemplu este cel al unei persoane (cont utilizator) care a acumulat în timp anumite privilegii acordate cu titlul temporar dar care nu i-au fost retrase, poate niciodată. Un caz similar este cel al persoanelor cărora li s-au schimbat sarcinile de serviciu sau au promovat şi care „cumulează" privilegiile vechi cu cele noi, acolo unde, în fond, nu ar fi de dorit aşa ceva.
Fizic	Măsurile aplicabile la nivel fizic se referă la posibilităţile de monitorizare (supraveghere) şi control al accesului persoanelor în clădire, în încăperile unde sunt depozitate sursele de informaţii şi – nu în ultimul rând – la calculatoare. Separarea sarcinilor este o regulă care merită avută în vedere. De exemplu, un programator nu ar trebui să fie în acelaşi timp şi administratorul unui server sau al unei baze de date: sunt roluri, respectiv responsabilităţi, care trebuie separate unele de altele.

Securitatea reţelelor este guvernată de trei principii fundamentale:

I. Apărarea în profunzime

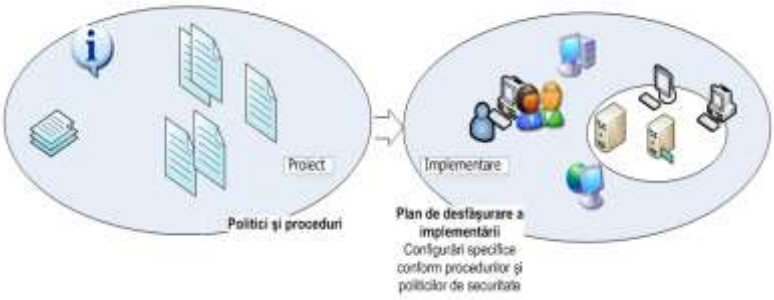
Apărarea în profunzime este definită drept o combinaţie de operaţii, persoane (execută operaţiile) şi tehnologii legate de securitate reţelei. Apărarea în profunzime presupune existenţa mai multor niveluri de apărare, de protecţie. Un singur nivel de protecţie este de cele mai multe ori insuficient. În eventualitatea existenţei mai multor straturi sau niveluri de protecţie, dacă unul dintre ele este spart, atunci cele rămase vor putea oferi pe mai departe protecţia necesară.

II. Privilegiul minim

Privilegiul minim este acordarea unui minim de privilegii pentru fiecare utilizator al resurselor reţelei. Privilegiile maxime induc vulnerabilităţi, potenţiale breşe de securitate care pot fi fructificate.

III. Minimizarea suprafeţei de atac

Minimizarea suprafeţei de atac se referă la existenţa unui număr cât mai mic de puncte care ar putea fi exploatate de un intrus „atacator”, fie el din interior sau din afară.



Securitate unei reţele se obţine prin implementarea unui proiect de securitate. Proiectul are în vedere construirea unei strategii de securitate, în care vor fi definite şi proiectate procedurile de securitate cele mai potrivite pentru protejarea reţelei. Implementarea acestor proceduri va asigura securitatea reţelei.

Bunurile care vor fi protejate prin aplicarea politicilor şi a procedurilor de securitate sunt plasate în locuri diferite şi se prezintă în forme diferite. Proiectul de securitate al reţelei va trebui să cuprindă politici şi proceduri care să protejeze fiecare arie de reţea faţă de ameninţările şi vulnerabilităţile identificate în aria respectivă.

Ameninţări

Ameninţarea este pericolul sau vulnerabilitatea care se poate materializa la un moment dat. Ameninţările vin din direcţii diferite: de la un „atacator” care ştie foarte bine ce vrea să obţină, de la aplicaţii prost sau insuficient configurate, de la utilizatori care îşi depăşesc îndatoririle. Ameninţările se materializează uneori în atacuri.

Atacurile au motivaţii din cele mai diverse: răzbunare, spionaj, publicitate, satisfacţie personală (inclusiv *hobby*), terorism.

Cele mai multe ameninţări, respectiv atacuri, survin pe fondul unor **vulnerabilităţi** comune, obişnuite:

- **parole slabe** – când nu se folosesc deloc parole, parolele folosite sunt cele implicite sau unele predictibile;
- **software neupgradat** – nu s-au aplicat corecţii de securitate (*patch*-uri) pentru vulnerabilităţi cunoscute;
- **hardware** şi **software incorect configurat** – utilizatorii au prea multe privilegii, aplicaţiile rulează folosind un cont sistem;
- **inginerii sociale** – dintre ingineriile sociale cea mai simplă este resetarea parolei de administrare sau a altei parole, ca urmare a unei cereri venite prin telefon de la o persoana căreia nu i se verifică identitatea;

- **securitate slabă la conexiunile la Internet** – porturile nefolosite nu sunt securizate, *router*, *switch*, *firewall* sunt folosite impropriu.
- **transfer necriptat** de date – pachetele ce compun operaţiile de autentificare circulă „în clar” în reţea sau date importante sunt transmise necriptat prin Internet.

De cele mai multe ori atacurile se desfăşoară respectând acelaşi model:

1. **amprentarea** – în acest stadiu atacatorul studiază reţeaua. Va obţine toate informaţiile public disponibile, despre organizaţie, conducere, angajaţi, va scana porturile pe toate calculatoarele la care poate ajunge, va accesa toate resursele disponibile prin Internet.
2. **penetrarea** – După identificarea şi localizarea vulnerabilităţilor urmează încercarea, testarea accesului la reţea şi la resursele din reţea. Cel mai expus loc: serverul de *web*.
3. **evaluarea privilegiilor** – după penetrarea reţelei are loc evaluarea privilegiilor: atacatorul încearcă să obţină privilegii de administrare sau de nivel „componentă a sistemului”. Eventual încearcă folosirea unui cont sistem pentru crearea unui cont nou de utilizator cu privilegii de administrare. De multe ori configurarea implicită îi lasă atacatorului suficientă libertate pentru a obţine acces în reţea fără prea mult efort.
4. **exploatarea** – după obţinerea privilegiilor necesare, atacatorul exploatează situaţia
5. **ştergerea urmelor** – în final atacatorul va încerca să-şi şteargă urmele spre a nu-i fi detectate acţiunile. Vor fi şterse conturile create şi intrările relevante din jurnale.

Posibilitatea de a anticipa ameninţările este de mare ajutor în identificarea şi implementarea regulilor de securitate care vor proteja reţeaua. Ameninţările se schimbă suficient de des, cel puţin în aceeaşi măsură în care se schimbă şi tehnologiile. Modelul ameninţărilor este tehnica folosită pentru anticiparea acţiunilor care ar putea fi întreprinse de un potenţial atacator în lipsa măsurilor de securitate. Modelul ameninţărilor este în fond o abordare structurată care identifică breşele de securitate, lacunele măsurilor de securitate aplicate la un moment dat. Ameninţările descoperite vor sta la baza planului de management al riscului: anticipând ameninţări posibile se poate opera în direcţia reducerii riscurilor. Pentru identificarea ameninţărilor la adresa securităţii reţelei şi a informaţiilor se vor folosi diagramele reţelei, informaţii despre configurările specifice ale calculatoarelor (hardware şi software) ca şi cele relative la configurarea aplicaţiilor. În plus, sunt de folos diagrame care identifică fluxul datelor / documentelor.

Ameninţările, oricare ar fi ele, respectă modelul STRIDE:

S T R I D E	
***S**poofing*	Păcăleală, înşelătorie
***T**ampering*	Falsificare, corupere
***R**epudiation*	Nerecunoaştere, renegare, refuz, negare
***I**nformation disclosure*	Divulgare, dezvăluire de informaţii
***D**enial of service*	Refuzarea serviciului
***E**levation of privilege*	Ridicarea, creşterea privilegiilor

Analiza riscurilor

Riscul este posibilitatea de a suferi o pierdere pentru care se calculează impactul, importanţa şi dimensiunea pagubelor care pot rezulta. Managementul riscului este procesul prin care sunt identificate şi analizate riscurile la care se adaugă planul de operaţii care previn riscurile şi reduc pagubele. Analiza riscurilor cuprinde o componentă calitativă şi una cantitativă.

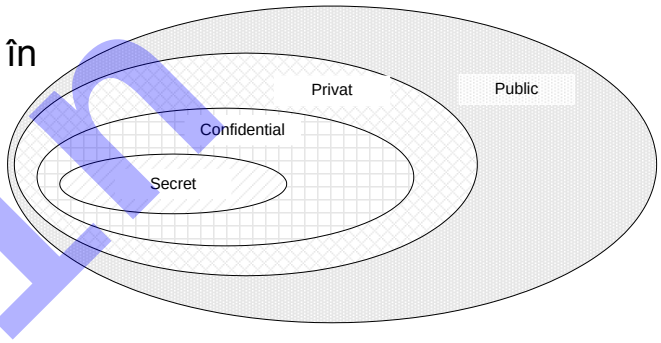
Analiza calitativă este cea care evaluează impactul şi importanţa pierderilor provocate. De cele mai multe ori, analiza calitativă are loc prin estimarea probabilităţii ca ameninţarea să se producă şi prin evaluarea importanţei, a impactului evenimentului. Înmulţind probabilitatea cu impactul (importanţa) se obţine riscul relativ, folosit în vederea ordonării riscurilor după priorităţi sau importanţă.

Analiza cantitativă se referă la măsurarea pagubelor, eventual exprimarea lor financiară. În aceeaşi categorie intră şi evaluarea costurilor necesare pentru reducerea probabilităţii de materializare a unei ameninţări şi respectiv, cele pentru diminuarea pagubelor.

Bunurile care au nevoie de protecţie prin aplicarea măsurilor de securitate sunt:

Tip	Exemple
Echipamente hardware	Calculatoare *desktop* şi *laptop*-uri Rutere şi *switch*-uri Mediile de comunicaţii şi cele folosite pentru salvări (*backup*)
Componente software	CD-uri sau DVD-uri folosite pentru instalarea sistemelor de operare şi a aplicaţiilor Imagini ale sistemelor de operare care pot fi transferate de la un calculator la altul Aplicaţii, fişiere cu comenzi, proceduri
Documentaţie	Politici şi proceduri legate de securitate şi de implementarea regulilor de securitate Diagrame şi planuri ale reţelei şi ale clădirilor unde este desfăşurată reţeaua
Date	Informaţii despre angajaţi Informaţii despre clienţi şi furnizori Orice alte informaţii specifice

Informaţiile folosite şi cele transmise în afară pot fi ordonate după gradul lor de expunere către exterior:



Strategie	Definiţie	Exemplu
Acceptare	Riscul există şi va fi acceptat ca atare	Nu va fi întreprins nimic special
Atenuare	Va fi redusă expunerea la risc	Împotriva viruşilor va fi folosit un produs antivirus
Transfer	Responsabilitatea asupra riscului va fi transferată măcar parţial asupra altei părţi	Pentru găzduirea unui *web site* va fi găsit un partener care să îşi asume ridcul
Eliminare	Riscul va fi eliminat, anulat prin eliminarea expunerii resursei	Oprirea din funcţiune a *site*-ului *web* dacă nu poate fi asigurată protecţia datelor confidenţiale

Schiţă de securitate pentru resurse fizice

Un atacator care are acces la resursele fizice – calculatoare, clădiri, încăperile serverelor – ar putea penetra foarte uşor reţeaua şi ar putea avea acces – în mod implicit – la informaţiile confidenţiale şi secretele organizaţiei. Securizarea accesului fizic necesită preocupare şi efort! Succesul protecţiei la nivelul resurselor fizice se traduce în fapt prin securizarea accesului la resurse. Protecţia software nu mai este suficientă dacă atacatorul are acces fizic la calculatoare sau la componentele reţelei. Din acest motiv vor fi protejate: clădiri, zone din interiorul clădirilor, conexiunile reţelelor, echipamentele hardware. Fără protecţie fizică, atacatorul ar putea încărca un program „cal troian" care să trimită caracterele tastate (în primul rând parole) undeva la o locaţie din Internet.

Ameninţările obişnuite la nivelul resurselor fizice sunt:

- Furtul calculatoarelor
- Instalarea aplicaţiilor subversive
- Sabotarea infrastructurii
- Instalarea de hardware şi / sau software de ascultare a reţelei şi urmărire a aplicaţiilor lansate în execuţie de angajaţi

Protejarea resurselor fizice are loc prin securizarea calculatoarelor din reţea şi a accesului la ele. Calculatoarele portabile au nevoie de un tratament special, fiind cele mai vulnerabile la furt şi sabotaj. Nu în ultimul rând ar trebui tratate pierderile datorate dezastrelor fizice: cutremure, incendii, inundaţii, vandalism, terorism, etc.

Există mai multe **metode de protecţie**; alegerea uneia sau a alteia se va face comparând costurile şi gradele de securitate obţinute prin diferitele metode:

- Angajarea paznicilor
- Folosirea ecusoanelor de identificare, a legitimaţiilor, insignelor, cardurilor de acces, etc.
- Supravegherea video
- Folosirea unei singure căi de acces atât pentru intrare cât şi pentru ieşirea din incinte, inclusiv clădirea principală
- Protejarea cablurilor pentru a nu fi ascultate sau redirecţionate
- Aşezarea monitoarelor şi a tastaturilor departe de ferestre
- Ştergerea tablelor din sălile de conferinţă, de întâlnire, de instruire, etc.
- Stabilirea unor reguli stricte în situaţia mutării calculatoarelor dintr-o reţea în alta

- Eliminarea din calculatoare a unităţilor de CD, DVD, şi a dischetelor
- instalarea de încuietori (lacăte)
- Restricţionarea accesului în camerele serverelor şi acolo unde sunt arhive
- Restricţionarea accesului la reţeaua locala LAN din spaţiile publice: holuri, secretariate, bufete, săli de conferinţă. etc.

Calculatoarele portabile, ca şi celelalte echipamente mobile, au nevoie de tratament şi atenţie speciale. Sunt folosite din ce în ce mai mult în vederea conectării la reţelele organizaţiilor şi la reţeaua Internet. Chiar dacă utilizatorii nu păstrează informaţii secrete pe aceste echipamente, ele pot deţine informaţii de autentificare ce ar putea fi exploatate de atacatori (ex.: nume de utilizatori şi parole, certificate). Calculatoarele portabile sunt dotate cu interfeţe *wireless* 802.11. Conexiunile *wireless* nesecurizate oferă vulnerabilităţi, mai ales în locuri publice aglomerate cum sunt aeroporturile, sălile de conferinţă, etc.

Planul **de recuperare** a datelor în urma incidentelor deosebite ar putea avea în vedere următoarele:

- Păstrarea seturilor *backup* în afară sediului organizaţiei
- Existenţa dublurilor pentru servere şi date (redundanţă)

Schiţă de securitate pentru computere

Ciclului de viaţă al unui calculator i se pot aplica modele de securitate, care să prevadă operaţii sigure şi corecte. Ameninţările la care sunt expuse calculatoarele pe durata ciclului de viaţă sunt:

- instalarea iniţială: lipsa protecţiei antivirus, configurări incorecte, parole slabe pentru conturile de administrare
- configurările iniţiale de securitate: folosind machete neverificate, machete implicite (ex. machetele implicite de tipul *Secutity Templates*)
- configurările suplimentare, în funcţie de rolul îndeplinit de calculatoare: ar putea fi incorecte, insuficiente, incomplet testate
- aplicarea actualizărilor de securitate pentru sistemele de operare şi aplicaţii: fără testări serioase
- încheierea activităţii: atenţie la echipamentele care păstrează informaţii, la hard discurile rămase şi care pot fi refolosite cu rea intenţie

Schiţa de securitate pentru calculatoare va face referire la toate stadiile ciclului de viaţă al calculatoarelor:

- instalarea va avea loc într-o reţea izolată de cea propriu-zisă
- vor fi făcute actualizări ori ce câte ori va fi nevoie: *upgrade*, *update* pentru „*service packs*”, „*patch*”, aplicaţii, produse antivirus
- regimul parolelor administratorilor va fi strict reglementat, la fel ca şi cel al tuturor utilizatorilor
- se vor folosi fişiere cu comenzi pentru instalarea şi configurare sistemelor de operare, a aplicaţiilor şi serviciilor
- vor fi folosite imagini sigure ale sistemelor de operare sau reinstalări ori de câte ori este nevoie
- se va folosi – dacă este posibil - RIS (*Remote Installation Service*) pentru instalarea şi configurarea automată a sistemelor de operare şi a aplicaţiilor
- instalarea, configurarea şi actualizările vor fi făcute de o persoană de încredere

Schiţă de securitate pentru conturile utilizatorilor

Conturile sunt folosite cu scopul de asigura accesul utilizatorilor la resursele reţelei. Numai utilizatorii cunoscuţi şi a căror identitate poate fi verificată vor avea acces la resursele reţelei. Fiecărui utilizator îi corespunde un cont utilizator şi o parolă. Dacă un intrus atacator obţine acces la un cont privilegiat atunci va obţine acces autorizat la resursele reţelei. Conturilor utilizatorilor le sunt asociate acţiunile pe care ei le pot întreprinde: utilizatori diferiţi au nevoie de reguli de securitate diferite:

- Utilizatori **externi** – utilizatori anonimi care au acces la serviciile *Web* cu aspect public, utilizatori *Web* autentificaţi, care au acces la *site*-urile *Web* protejate, utilizatori parteneri
- Utilizatori **interni** – angajaţi şi conducere (personalul organizaţiei), de cele mai multe ori utilizatori neprivilegiaţi
- Administratori – utilizatori cu privilegii administrative, conturi folosite de servicii, aplicaţii, componente sistem, administratori ai datelor, administratori ai serviciilor

Conturile utilizatorilor dobândesc privilegii din următoarele surse:

- Drepturi – „*user rights*”
- Permisiuni la resurse (ACL, DACL)
- Aria de vizibilitate - conturi locale, conturi în domeniu
- Apartenenţa la grupuri

Privite astfel **vulnerabilităţile principale** ale conturilor sunt:

- **Parolele** – prea slabe, identice pentru mai multe conturi, nemodificate la timp, păstrate local, scrise pe hârtie şi uitate
- **Privilegii** – prea mari şi prea multe pentru utilizatori în raport cu sarcinile şi acţiunile lor
- **Folosirea conturilor** – contul Administrator folosit atunci când nu este nevoie, conturi active chiar dacă nu mai sunt folosite

Schiţa de securitate pentru conturi, inclusiv cele din domeniu, se va construi pornind de la premiza că fiecărui cont îi sunt asociate **numai** acele privilegii care îi sunt strict necesare. În acelaşi timp, fiecare cont va fi folosit numai în scopul pentru care a fost creat.

- A_G_DL_P (*Account, Global Group, Domain Local, Permissions*) este modelul preferat de Microsoft pentru asocierea permisiunilor în domeniu.
- La asigurarea drepturilor şi a permisiunilor se vor folosi „rolurile” îndeplinite de persoane în organizaţie.
- Pentru păstrarea consistenţei grupurilor se va folosi „*Restricted Groups*”
- Securitatea va fi controlată şi gestionată centralizat

Pentru construirea schemei de securitate sunt importante nivelurile de încredere acordate utilizatorilor (persoane), respectiv:

- Cine gestionează conturile şi parolele?
- Cine obţine informaţii despre conturi şi respectiv cine cunoaşte informaţiile înscrise în conturile utilizatorilor?

În general, se recomandă crearea unor proceduri bine descrise şi structurate (eventual chiar fişiere *script*) pentru:

- crearea / ştergerea conturilor, distribuirea parolelor, monitorizarea creării noilor conturi şi a blocării / ştergerii celor nefolosite.
- atribuirea drepturilor şi a permisiunilor

În plus, administratorii vor fi atenţi la: apartenenţa la grupuri (*Restricted groups*), folosirea conturilor administrative şi a condiţiilor în care sunt folosite conturile cu privilegii administrative. Se recomandă folosirea pentru administrare a procedurilor ***Terminal Service*** **în mod** ***Remote Administration*** sau a modului de lucru **„*runas*…”.**

Schiţă de securitate pentru autentificarea utilizatorilor

Autentificarea validează corectitudinea informaţiilor de acreditare („*credentials*”) pe care le posedă un utilizator. Pentru reţelele Microsoft Windows, metodele de autentificare diferă în funcţie de locul şi modul în care un cont accesează reţeaua.

Proiectul de securitate referitor la autentificare va trata toate tipurile de autentificări folosite în reţea, inclusiv aplicaţiile care folosesc propriile protocoale de autentificare. Autentificările sunt diferite în funcţie de modul în care utilizatorul se conectează la reţeaua locală LAN: direct, de la distanţă („*remote*”), sau prin Internet.

Vulnerabilităţile cele mai cunoscute sunt:

- parole transmise în clar (necriptat)
- parole interceptate de programele „cal troian”
- software mai vechi care foloseşte metode slabe de autentificare
- criptări slabe
- interceptarea pachetelor de autentificare

Cerinţele de autentificare vor fi determinate pornind de la:

1) identificarea cerinţelor de autentificare în funcţie de sistemul de operare folosit (Windows 95, Windows 98, Windows XP, 2000, Windows Vista, Windows 7, etc.)
2) identificarea cerinţelor de compatibilitate ale aplicaţiilor
3) strategia impusă pentru autentificare

Protocoalele folosite de sistemele de operare Microsoft Windows pentru autentificare sunt:

LAN Manager	Folosit de sisteme de operare mai vechi; Nesigur; Foloseşte „*challenge and response*”;
NTLM	Folosit de sistemul de operare Windows NT 4.0; Folosit de sistemele de operare Windows 2000 si următoarele pentru conturile locale; Foloseşte „*challenge and response*”;

NTLM v.2	Apare la Windows 95 şi următoarele; Este un NTLM mai sigur, prin adăugarea securităţii la nivel de sesiune şi a criptării; Autentifică mutual clientul şi serverul;
Kerberos	Folosit pentru conturile din domeniu, începând cu Windows 2000: Autentifică mutual clientul şi serverul; Acceptă „*smart card*”;

Serviciul IIS 5.0 (*Web*) este responsabil de autentificarea utilizatorilor în următoarele **condiţii:**

anonim	Permite accesul utilizatorilor la *site*-ul *Web* fără să fie necesară prezentarea informaţiilor de acreditare, şi anume fără ca utilizatorul să se identifice prin nume şi parolă. Toţi utilizatorii anonimi vor fi în fapt autentificaţi drept IUSR_NumeServer.
de bază („*basic*”)	Trimite numele şi parola în clar prin reţea (necodificat, necriptat). Ca să poată folosi acest mod de autentificare, utilizatorul trebuie să poată face *log on* local la serverul IIS. Toate *browser*-ele *Web* admit autentificarea „*basic*”; poate fi folosită şi cu servere *proxy*. Se recomandă folosirea acestei forme de autentificare numai împreună cu SSL(*Secure Socket Layer*).
prin rezumat („*digest*”)	Foloseşte nume şi parolă la care se adaugă o valoare aleatoare pentru crearea unui „*hash*” care va îmbunătăţi autentificarea în model „*basic*”. Serverul IIS trebuie să fie membru al domeniului; conturile utilizatorilor din domeniu care vor avea acces la *site* au proprietatea „parole păstrate în *Active Directory* folosind criptarea reversibilă” (*reversible encryption*).

integrat Windows	Un calculator pe care rulează IE 4.0 sau superior asigură automat autentificarea utilizatorului: sunt folosite numele şi parola păstrate în „*cache*. Implicit IIS 5.0 foloseşte Kerberos, dar va folosi şi NTLM dacă autentificarea prin Kerberos eşuează. Nu poate fi folosit cu *proxy*.
Prin certificate	Utilizatorul sau calculatorul se vor autentifica la serverul *Web* prin folosirea unei chei private asociate certificatului X509. Certificatul este asociat („*map*”) unui cont utilizator local sau din domeniu. Este cea mai sigură metodă de autentificare pentru serverele IIS 5.0

Autentificarea utilizatorilor aflaţi la distanţă (*remote*) este necesară în condiţiile folosirii conexiunilor prin **linii telefonice** (*dial-up*) sau prin **VPN** (*Virtual Private Network* – reţea virtual privată). Pot fi folosite **următoarele protocoale de autentificare**:

CHAP	*Challange Handshake Authentication Protocol*, protocol de autentificare de tipul *„challenge response”*. Foloseşte pentru „*hash*” algoritmul *Message Digest 5* (MD5); *Hash=a şopti, a tăcea, a sta liniştit;* acest algoritm codifică răspunsul la provocarea pe care o lansează serverul aflat la distanţă (fată de utilizator). Parola trebuie păstrată în *Active Directory* folosind criptarea reversibilă (*reversible encryption*), ceea ce introduce vulnerabilităţi. Pe de altă parte, CHAP nu permite criptarea datelor.
MS-CHAP	Similar cu CHAP; nu cere ca parola să fie accesibilă prin criptare reversibilă.
MS-CHAP v.2	Include: autentificarea mutuală, chei separate pentru trimitere şi recepţionare, chei de sesiune generate automat, pornind de la parola utilizatorului.

EAP-TLS	*Extensible Authentication Protocol – Transport Layer Security*; oferă: autentificare, integritatea datelor, confidenţialitate; foloseşte autentificarea mutuală, negocierea algoritmilor de criptare; transmiterea / recepţionarea cheilor de sesiune este sigură; este asigurată integritatea mesajului. Poate fi folosit împreună cu cardurile „*smart card*” şi este cel mai sigur protocol de autentificare.

Autentificarea multifactor este tipul de autentificare prin care i se cere utilizatorului să ofere mai multe informaţii de acreditare (*credentials*), cum ar fi: coduri de acces (PIN) , componente fizice (chei, jetoane), informaţii biometrice individuale (voce, amprente). Autentificarea multifactor creşte siguranţa accesului şi a lucrului în reţea. Este recomandată mai ales pentru utilizatorii de la distanţă, acolo unde verificarea identităţii lor nu este posibilă. Este evidentă utilitatea acestor metode pentru conturile care au privilegii de administrare, ca nivel suplimentar de securitate.

Schiţă de securitate pentru date

Securitatea datelor se defineşte şi prin controlul asupra modului în care are loc accesul la date. Controlul se exercită prin asignarea permisiunilor. Potenţialii atacatori ar putea, în anumite condiţii, să suprascrie permisiunile pentru a controla ei accesul la date. Pentru controlul accesului la resurse se folosesc două tipuri de informaţii: jetoanele software de acces ale utilizatorilor şi listele DACL/ACL (*Discretionary Access Control List*): jetoanele indică în general **drepturile** utilizatorilor, DACL/ACL arată **permisiunile** la obiectele din *Active Directory* şi la cele din sistemul de fişiere NTFS, respectiv, dosare şi fişiere.

Când utilizatorul este autentificat, calculatorul pe care acesta îl foloseşte va primi şi va păstra un jeton care conţine: identificatorul de securitate al contului utilizatorului (SID), identificatorii SID ai fiecărui grup (local sau din domeniu) din care face parte utilizatorul şi lista drepturilor de care dispune (*user rights*). În situaţia accesului la o resursă, SID-urile din jeton se compară cu cele DACL/ACL asociate resursei.

Datele (informaţiile) dintr-o organizaţie sunt vulnerabile faţă de ameninţări interne şi externe, provenite de cele mai multe ori prin:

- incorecta configurare a permisiunilor
- insuficienta securitate fizică a datelor şi a accesului la suporturile de date
- stricăciuni aduse datelor (alterare, criptare incorectă)

Configurarea – la nivel fizic şi logic – a securităţii datelor va începe întotdeauna de la asigurarea minimului de permisiuni de acces la date pentru toţi utilizatorii, respectiv pentru fiecare dintre ei: utilizatorii vor avea un **minim de permisiuni, suficient** numai pentru exercitarea atribuţiilor de serviciu.

A_G_DL_P este un modelul folosit pentru implementarea securităţii pornind de la rolurile îndeplinite de utilizatori într-o organizaţie. Modelul plasează conturi în grupuri, grupurile în alte grupuri (locale domeniului) şi le asociază acestora din urmă permisiuni şi – dacă este cazul – drepturi.

Permisiunile NTFS funcţionează când un utilizator accesează resurse aflate pe un volum NTFS; volumul poate fi local sau la distanţă. Permisiunile de partajare au efect când este vorba de date aflate în reţea, la distanţă faţă de utilizator.

Toate obiectele – dosare şi fişiere – aflate în componenţa unui volum NTFS au un proprietar, care are întotdeauna permisiunea de a controla permisiunile asociate acelei resurse. Această posibilitate a proprietarului ar putea fi o armă subversivă în politica de securitate.

Efs – *encrypted file system* – este un instrument puternic în protejarea şi siguranţa datelor. Folosit incorect însă, poate face ca utilizatori legitimi să nu mai poată avea acces la datele de care au nevoie. Acolo unde există politici referitoare la criptarea datelor trebuie să existe şi unele pentru recuperarea datelor criptate.

Schiţa de securitate a transmisiei de date

Datele sunt vulnerabile şi pe timpul transmiterii; vulnerabilităţile cele mai cunoscute în această situaţie sunt legate de execuţia a unor operaţii răuvoitoare:

Monitorizarea neautorizată a reţelei şi a traficului de date din reţea	Observarea traficului de autentificare Citirea pachetelor *e-mail* Observarea traficului de management Citirea pachetelor de criptare *wireless*
Păcălală (*Spoofing*)	Identificarea şi folosirea abuzivă a adreselor IP pentru a face ca pachetele să pară a fi transmise din reţeaua locală Falsificarea pachetelor ICMP Trimiterea de *e-mail*-uri falsificate
Modificarea (alterarea) datelor	Interceptarea şi modificarea datelor
Denial of service (negarea serviciului)	Inundarea unui calculator / serviciu cu mesaje Folosirea mai multor calculatoare care trimit mesaje inundând reţeaua.

Schiţa de securitate pentru transmiterea datelor are ca punct de plecare securizarea comunicaţiilor prin reţea, nivelurile modelului cu patru straturi (niveluri) implementat de protocolul TCP/IP. Fiecare nivel este vulnerabil în felul său; pe de altă parte nu tot traficul trebuie securizat întotdeauna.

	Metode de securizare recomandate
aplicaţie	*Secure Socket Layer* (SSL), *Transport Layer Security* (TLS), S/MIME (*Security Multiuse Internet Mail Extensions*, 802.1x
reţea	IPSec Tunel IPSec
Legătura de date	*Switch*-uri în loc de *hub*-uri Autentificare la nivel de port
fizic	Securitate strictă la nivel fizic: încăperi, cabluri, echipamente, incinte Restricţii de acces la reţeaua LAN din zone de acces public

Securitatea reţelei perimetru

Terminologia din domeniul securităţii reţelelor de calculatoare include termenul de zonă demilitarizată sau DMZ (*demilitarized zone*). DMZ este o subreţea fizică sau logică care conţine servicii cu vizibilitate externă: servere de *web*, de *mail*, servere DNS. Reţeaua DMZ se mai numeşte şi reţeaua perimetru, cu înţelesul că restul reţelei, rămas după decuparea zonei DMZ, este protejat, marcat printr-o frontieră de securitate. Scopul existenţei reţelelor DMZ sau perimetru este cel de a adăuga un nivel suplimentar de securitate pentru reţeaua LAN a unei organizaţii. Componentele din DMZ şi numai ele sunt expuse către exterior. Pachetele de date dintre reţeaua DMZ şi reţeaua LAN vor fi filtrate pentru ca restul reţelei să fie protejat de eventualele intruziuni ale atacatorilor. Filtrele vor asigura comunicaţia limitată, strict controlată, dintre componentele DMZ şi componentele reţelei LAN. Rolul de legătură intre reţeaua DMZ şi Internet, pe de o parte, şi reţeaua LAN pe de altă parte este îndeplinit de serviciile *firewall*.

Reţeaua perimetru (DMZ) conţine:

- conexiunile directe la Internet
- legături WAN dedicate

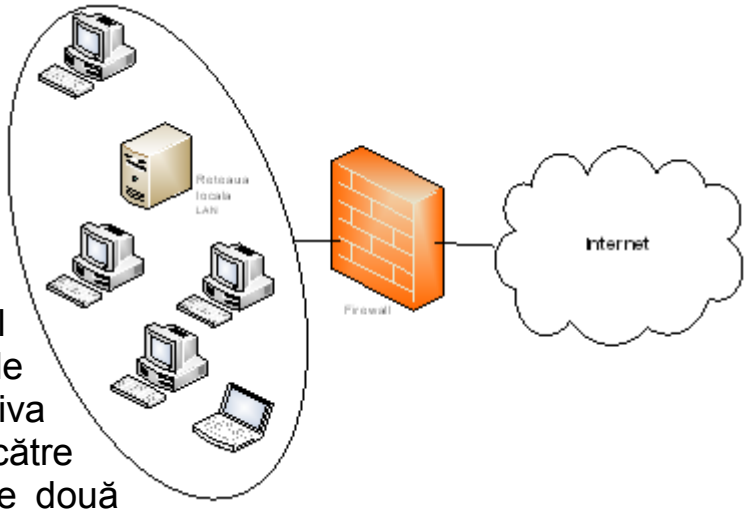
- subreţele ecranate, zone protejate special pentru că sunt expuse accesului din reţele publice
- clienţi VPN
- conexiuni *wireless*

Vulnerabilităţile cunoscute provin din aceea că **perimetrul este zona cu cea mai mare expunere** la **reţelele publice: Internet, acces de la distanţă, conexiuni cu birouri (filiale, sucursale) aflate la distanţă.** Vulnerabilităţile apar prin:

- expunerea intenţionată sau neintenţionată a informaţiilor despre reţea: scanarea porturilor, TCP/UDP, scanarea perimetrului ICMP, analiza pachetelor
- controlul incomplet asupra infrastructurii: servere Web neautorizate, conexiuni uitate, clienţi VPN necontrolaţi, aplicaţii necontrolate
- expunerea voluntară sau involuntară a calculatoarelor: urmările sunt atacuri asupra serviciilor, expunerea informaţiilor despre conturi, viermi *e-mail*, acces neautorizat la date, distrugerea datelor.

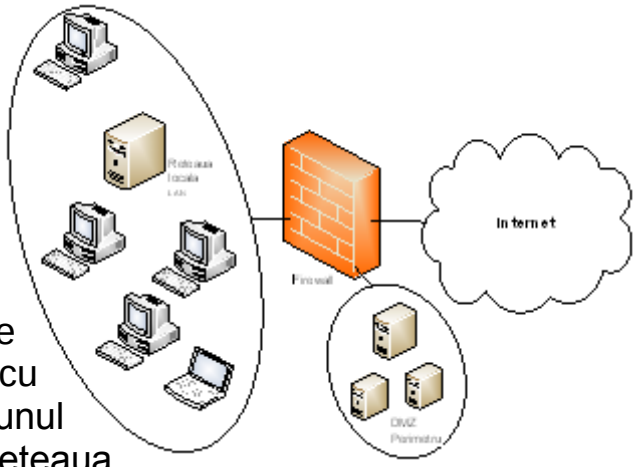
Perimetrul este, prin definiţie, un loc unde încrederea este limitată: se presupune că zona nu este sigură, că poate fi oricând atacată. Securitatea perimetrului se construieşte cu un **„*firewall*”** sau **paravan de securitate** şi cu echipamente hardware specializate. Soluţia Microsoft pentru servicii de tip *firewall* este serverul *Internet Security and Acceleration Server* (ISA)

Există următoarele tipuri de configurare a serverului *firewall*, respectiv de constituire a perimetrului:

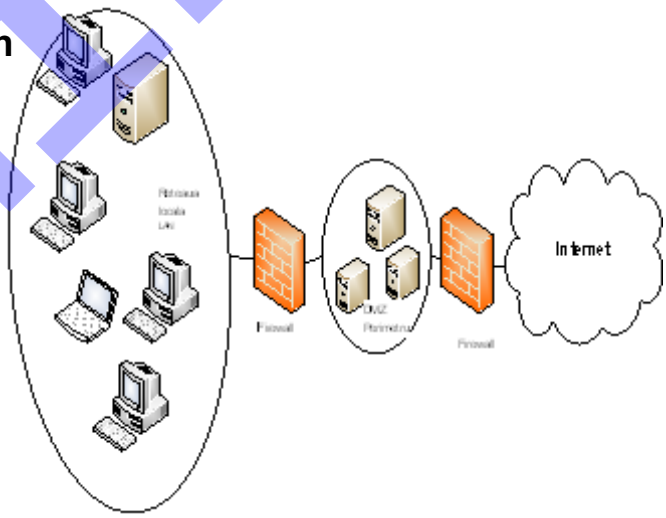


- **„host bastion”** – serverul *firewall* este conexiunea principală pentru accesul la Internet al calculatoarelor din reţeaua internă. Ca *firewall*, calculatorul bastion este proiectat să le apere pe celelalte împotriva atacurilor direcţionate către interior. Bastionul foloseşte două adaptoare de reţea: unul conectat la reţeaua internă, unul la reţeaua Internet. Această configuraţie izolează fizic reţeaua internă de intruşii din Internet.

- **Configuraţie „cu trei dinţi”** numită câteodată şi cu „trei picioare” - oferă utilizatorilor din Internet acces limitat la resursele reţelei, interzicând traficul nedorit cu calculatoarele din LAN. Se foloseşte un *firewall* cu trei adaptoare de reţea: unul conectat la LAN, unul la reţeaua ecranată, protejată (alta decât LAN) şi al treilea la Internet. Izolează traficul intern şi reţeaua internă de Internet şi permite accesul limitat din Internet şi din reţeaua locală la reţeaua ecranată.



- **Configuraţie „spate în spate” –** plasează subreţeaua ecranată între două *firewall*-uri: unul conectat la Internet, celălalt la reţeaua locală, internă. Există un singur punct de acces din Internet la reţeaua locală şi acela cere să treci prin două *firewall*-uri.



Mecanismele de securitate implementate prin serviciile *firewall* sunt:

- Filtrarea pachetelor
- Reguli noi de rutare a pachetelor
- Inspecţia stării pachetelor
- *Gateway* între aplicaţii
- Servicii publicate şi care devin astfel disponibile – în condiţii controlate – din reţeaua Internet
- Autentificarea utilizatorilor în vederea accesului către exterior, către reţeaua Internet
- Detectarea intruşilor, respectiv utilizatori din afară care încearcă acces la resursele protejate prin *firewall*

Reacţii la apariţia incidentelor de securitate

Securitatea reţelelor este în fond un exerciţiu de prevenire: evenimentele majore ar putea să nu apară, dacă activitatea de prevenire a avut loc şi dacă toate procedurile stabilite au fost aplicate corect. De multe ori însă, apărarea proiectată este străpunsă de atacatori. În urma unui atac nu mai rămân decât minimizarea pagubelor, aprecierea rapidă a urmărilor şi răspunsul la apariţia incidentului. Procedura de răspuns se compune din paşii de urmat **după** apariţia incidentului.

Auditul este modalitatea prin care se pot înregistra (înscrie, păstra) evenimentele petrecute deja. Jurnalele acestor evenimente pot releva informaţii despre atacuri întreprinse asupra resurselor reţelei.

Politica de audit a unei organizaţii trebuie să includă răspunsuri la următoarele întrebări:

- Ce tipuri de evenimente vor fi supravegheate (*audit*)?
- Ce instrumente de audit se vor folosi?
- Cum vor fi investigate evenimentele care au trezit suspiciuni?
- Cât timp vor fi păstrate jurnalele?
- Cine analizează evenimentele şi cât de des?
- Cum să fie păstrate dovezile?

Procedura de răspuns la incidente conţine paşii şi acţiunile de întreprins **după** apariţia incidentului. Scopul existenţei procedurii este limitarea pagubelor şi încercarea de a răspunde organizat, controlat şi eficient la un incident petrecut anterior.

Planul de declanşare a răspunsului este o activitate organizatorică care cuprinde – la rândul ei – mai mulţi paşi:

1) Constituirea şi instruirea echipei care gestionează răspunsurile la incidente;
2) Dezvoltarea planului de comunicare: între membrii echipei şi cu ceilalţi angajaţi;
3) Construirea planului de identificare a atacului şi, dacă este posibil, a atacatorului;
4) Construirea şi revizuirea periodică a politicilor;
5) Documentarea incidentelor – după apariţia lor;

Răspunsul la incidente va fi temeinic pregătit pentru a putea acţiona deplin şi eficient. Primul şi cel mai important aspect al răspunsului va fi protejarea şi siguranţa vieţii oamenilor. Abia după aceea va fi vorba despre: protejarea

informaţiilor secrete, a celor confidenţiale, a altor informaţii, protejarea componentelor hardware şi a celor software. La sfârşit se va avea în vedere minimizarea pagubelor.

Echipa însărcinată cu stabilirea şi declanşarea răspunsurilor la incidente de securitate va fi compusă din cât mai puţini membri, pentru a asigura rapiditate şi eficienţă în declanşarea acţiunilor. În general, membrii acestei echipe ar trebui să poată îndeplini următoarele roluri:

specialist în securitate	evaluează şi investighează incidentele de securitate; oferă sfaturi şi soluţii
administrator reţelei	oferă informaţii despre configuraţia reţelei şi a calculatoarelor; participă la evaluarea pagubelor;
conducere	ia decizii critice, de la caz la caz, privind răspunsurile la incidente şi măsura în care incidentele vor fi făcute publice;
consilier pentru probleme legislative	sfătuieşte conducerea cu privire la acţiunile judiciare şi condiţiile de desfăşurare;

Indiciile apariţiei incidentelor de securitate sunt diferite şi nu întotdeauna sigure. Semne asociate posibilelor incidente pot proveni din mai multe locuri, ca de ex.:

- Scăderea performanţelor reţelei şi a sistemelor în general;
- Calculatoare care „cad” şi se restartează misterios;
- Conturi de utilizator folosite în condiţii şi la momente cel puţin ciudate;
- Creşterea numărului de evenimente de audit înregistrate într-un interval de timp;
- Utilizatorii raportează incidente;
- Apar informaţii despre un nou virus;
- Software-ul specializat detectează „intruşi”;

După detectare**, incidentul va fi analizat**. Cele mai importante informaţii ce vor fi obţinute prin analiză sunt:

- **Simptomele** – cum a apărut şi cum se manifestă atacul;
- **Originea** – care este punctul de origine şi dacă se poate face o legătură între originea incidentului şi un prezumtiv atacator;

- **Punctul de intrare** – cum şi pe unde a pătruns atacul, eventul dacă exploatează o vulnerabilitate cunoscută;
- **Intenţia** – ce intenţionează atacatorul să obţină şi dacă foloseşte vreun model pentru desfăşurarea atacului;
- **Gravitatea** – care sunt riscurile şi cât de grave sunt, sau ar putea fi mai târziu impactul şi /sau pagubele;
- **Expunerea** – ce sisteme au fost compromise prin expunerea la atac şi în ce constau pagubele

Limitarea **pagubelor** ar trebui să fie răspunsul imediat şi prompt:

- Deconectarea de la reţea a calculatoarelor (echipamentelor) afectate şi a celor care deţin date importante;
- Deconectarea organizaţiei de la Internet, blocarea unor porturi TCP / UDP;
- Instalarea de componente de actualizare „*upgrade*”, „*patch*”, antivirus, componente pentru detectarea intruşilor;
- Schimbarea parolelor pentru utilizatori;
- Schimbarea cheilor software;
- Schimbarea componentelor de protecţie fizică: încuietori, lacăte, chei, carduri de acces, etc.

După rezolvare, incidentul va fi documentat cu minuţiozitate. Toate informaţiile obţinute prin analiză vor fi sistematizate spre a fi apoi introduse în noile politici şi proceduri de securitate, dacă este cazul.

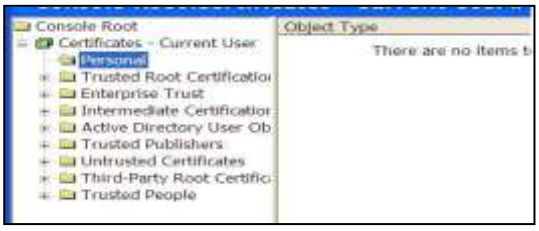
MBSA (Microsoft Baseline Security Analyzer)

Microsoft *Baseline Security Analyzer* este unul dintre programele folosite pentru identificarea problemelor legate de securitate şi a actualizărilor de securitate necesare unui computer unde rulează un sistem de operare Microsoft. MBSA scanează configuraţia hardware şi software existentă, identifică posibilele breşe de securitate şi indică operaţiile de executat în acest sens, inclusiv actualizările de care are nevoie sistemul. MBSA poate fi descărcat gratuit de pe *site*-ul Microsoft.

Câteva soluţii Microsoft pentru securitatea reţelelor

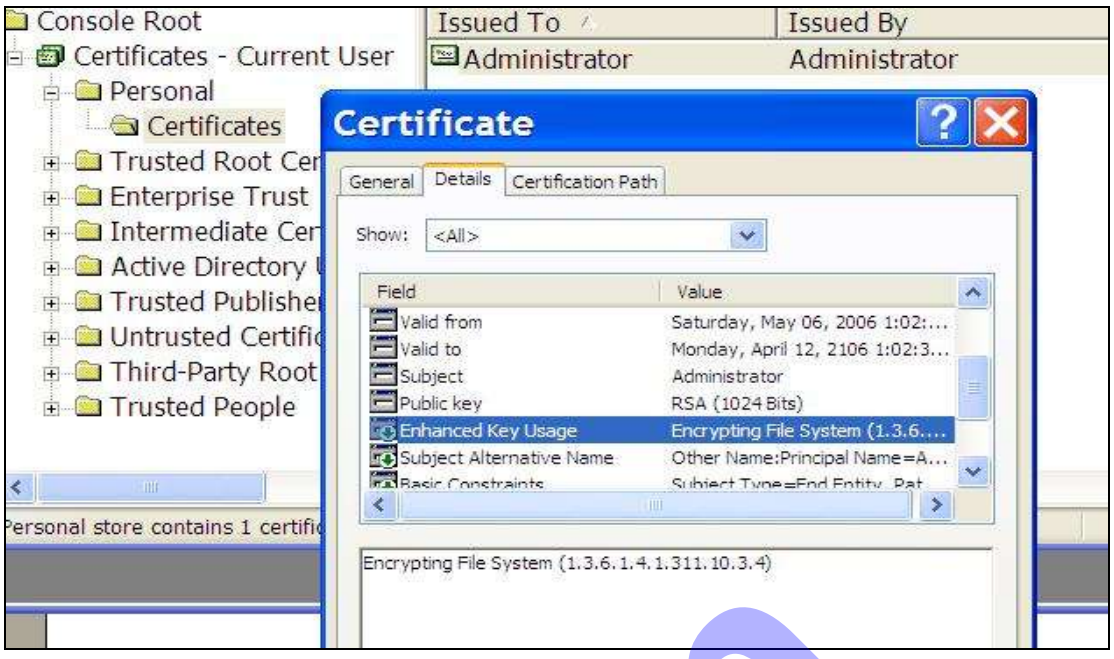
EFS - Encrypting File System

Encrypting File System este soluţia pentru păstrarea sigură a datelor pe hard discuri formatate NTFS. EFS permite utilizatorilor să-şi cripteze propriile fişiere. Criptarea şi decriptatea fişierelor se face prin folosirea unui certificat special destinat acestui scop.



1. Când un utilizator criptează un fişier pentru prima data, EFS verifică dacă există în *local certificate store* un certificat care poate fi utilizat pentru EFS.

2. În situaţia în care un astfel de certificat nu există, EFS va lansa o cerere pentru un certificat de tip EFS. Cererea este în mod tradiţional adresată unei autorităţi de certificare. Dacă în reţea nu funcţionează niciun server care poate elibera certificate, atunci certificatul va fi generat local de către sistemul de operare.

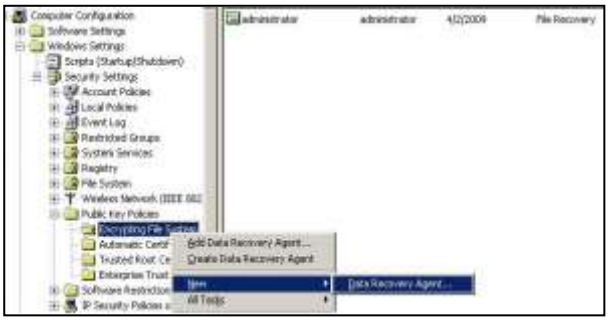


Se generează în continuare un număr aleator numit *File Encryption Key* (FEK), cheia pentru criptarea fişierului. Caracteristicile acestei chei sunt dependente de sistemul de operare.

Operating System	EFS Algorithm	Key Strength
Windows Server 2003	AES	256 bit
Windows XP	DESX	128 bit
Windows XP SP1 or later	AES	256 bit
Windows 2000	DES	56 bit
Windows 2000 SP2 or later or with High Encryption Pack	DESX	128 bit

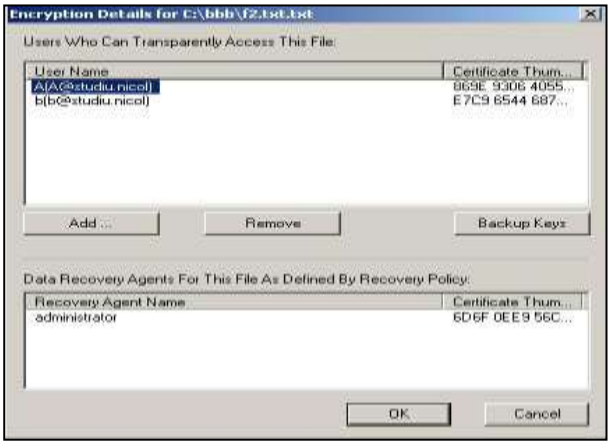
3. EFS preia cheia publică şi criptează fişierul.

Recuperarea fişierelor, în cazul în care certificatul utilizatorului devine inaccesibil (de ex. a fost şters profilul utilizatorului sau i-a fost modificată parola), poate fi făcută de agentul recuperator *(Recovery Agent)*. Agentul recuperator foloseşte un certificat adecvat care îi permite să decripteze fişiere pe care nu le-a criptat.



Certificatul agentului recuperator poate fi obţinut de la o autoritate de cerificare sau poate fi generat local, de către sistemul de operare.

În situaţia existenţei unui domeniu *Active Directory*, obiectele *Group Policy Object* (GPO) pot fi folosite pentru stabilirea agentului recuperator. Administratorul de domeniu este în mod implicit agentul recuperator. Cheia privată a administratorului de domeniu (agent recuperator) se află pe primul controler de domeniu creat. Această cheie trebuie importată de la controlerul de domeniu şi folosită pe calculatorul unde se află fişierul de recuperat.



EFS file sharing este o facilitate a sistemelor de operare Windows XP şi Windows Server 2003 şi permite partajarea accesului la un fişier criptat, intre mai mulţi utilizatori.

Securitatea unui server membru in domeniu

Securitatea unei reţele depinde de setările de securitate realizate pentru fiecare din serverele din reţea. O breşă de securitate la un singur server poate compromite întreaga reţea.

Pentru a menţine un mediu securizat vor fi avute în vedere următoarele soluţii:

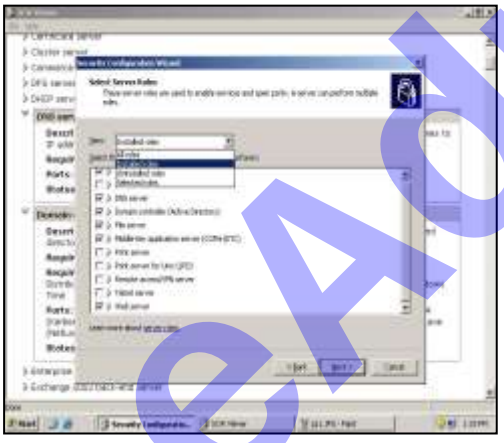
- aplicarea ultimului *service pack* şi a actualizărilor de securitate (*security updates*) disponibile
- folosirea politicilor *Group Policy* pentru:
  - dezactivarea serviciilor care nu sunt necesare. Orice serviciu care rulează poate reprezentă un potenţial punct de atac. Cu atât mai mult unul nefolosit niciodată.
  - implementarea de politici pentru parole securizate, utilizarea de parole cât mai complexe (in nici un caz folosirea de parole vide !!)
  - dezactivarea LAN Manager şi a autentificării de tip NTLM v1, în cazul în care nu sunt absolut necesare; autentificarea NTLM v1 este folosită la sistemele de operare ceva mai vechi
  - restricţionarea dreptului de deschidere a unei sesiuni locale la un server *(Log on locally)*
- folosirea utilitarului *Microsoft Baseline Security Analyzer* (MBSA) pentru scanarea configuraţiilor aflate în funcţiune şi identificarea posibilelor probleme de securitate

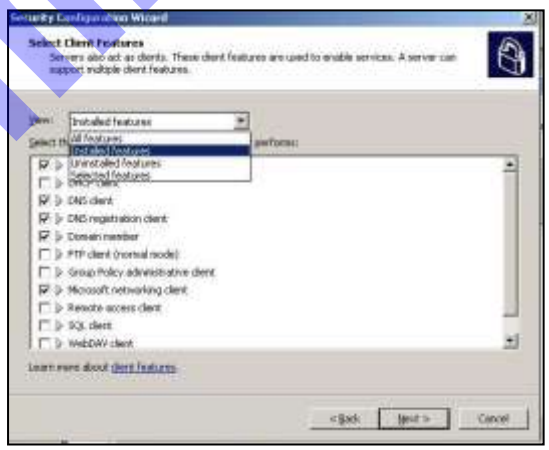
- restricţionarea accesului fizic la servere, prin plasarea lor in camere încuiate sau bine păzite
- securizarea contului de administrator, de ex., prin folosirea parolelor diferite pentru fiecare administrator local al fiecărui server, restricţionarea grupurilor cu drepturi administrative prin utilizarea de *Restricted Groups*, redenumirea contului de administrator
- separarea conturilor de utilizator şi a celor cu privilegii administrative: niciodată un cont cu privilegii de administrare nu va fi folosit pentru operaţii uzuale (*mail*, rularea aplicaţiilor standard, navigare pe Internet). Va fi folosit *Secondary Logon* (*run as*…) pentru administrare, atunci când este posibil.
- folosirea permisiunilor NTFS pentru securizarea folderelor şi a fişierelor
- stabilirea unei politici de audit pentru detectarea modificărilor care pot apărea la nivelul configurărilor care au legătură cu securitatea
- restricţionarea accesului la serverele din reţeaua locală folosind *Windows Firewall*, eventual configurarea lor centralizată prin folosirea GPO
- crearea unei structuri de unităţi organizaţionale in *Active Directory* care să permită construirea şi legarea corespunzătoare a obiectelor GPO necesare
- utilizarea machetelor de securitate (*security template*) pentru configurarea regulilor de securitate. Testarea regulilor de securitate înainte de aplicarea lor in mediul real
- asigurarea sincronizării timpului, având în vedere că protocolul *Kerberos* nu permite autentificarea dacă diferenţa de timp între client şi server este mai mare de 5 minute. Serviciul W32Time asigură sincronizarea dintre serverele membre ale domeniului şi controlerul de domeniu, utilizând protocolul *Network Time Protocol* (NTP)
- se recomandă folosirea unui *smart card* pentru deschiderea de sesiune, ca administrator
- restricţionarea staţiilor de unde poate deschide sesiune administratorul
- evitarea rulării pe controlerul de domeniu a altor servicii decât cele strict necesare în funcţionarea unui controler de domeniu. Se recomandă ca administrarea domeniului să se facă de la un alt calculator membru al domeniului, evitându-se deschiderea de sesiune efectuată chiar de la controlerul de domeniu.
- crearea de grupuri administrative cu drepturi specifice pentru executarea unor anumite operaţii bine determinare cum ar fi:

administrator de OU, administrator de server DNS, server WINS, DHCP etc.

Utilitarul Security Configuration Wizard

Security Configuration Wizard (SCW) este componenta folosită pentru configurarea rapidă a serverelor, în funcţie de cerinţele de funcţionalitate (*Web* server, *domain controller*, DNS, etc.). Prin programul *Security Configuration Wizard* se pot dezactiva serviciile care nu sunt necesare, se pot bloca porturi, se poate modifica conţinutul din regiştrii (*registry*). Configurările operate pot fi salvate într-un fişier, de unde vor fi aplicate ulterior. Acelaşi fişier poate fi folosit pentru configurarea mai multor calculatoare.





Servere securizate in funcţie de rolul în reţea

- ✓ **controlerul de domeniu**:
  - va fi plasat într-un loc sigur, la care să nu aibă acces decât personalul autorizat
  - se recomandă să existe cel puţin două controlere de domeniu, pentru siguranţă
  - se recomandă replicarea securizată a traficului DNS asociat, folosind IPSec sau replicarea *Active Directory,* pentru situaţia în care zona DNS este inclusă în AD
  - se recomandă redimensionarea jurnalelor *event log,* pentru păstrarea a cat mai multe informaţii in cazul unui atac (16 MB)
  - se recomandă păstrarea bazei de date *Active Directory* şi a fişierelor jurnal *(log)* asociate în locuri diferite, eventual pe un discuri separate
  - se recomandă dezactivarea serviciilor nenecesare şi blocarea porturilor nefolosite
  - urmărirea evenimentelor se va face prin procedurile de audit. Recomandările minimale sunt cele din tabelul de mai jos:

Audit policy	Setari minimale recomandate
Audit account logon events	*Success, Failure*
Audit account management	*Success, Failure*
Audit directory service access	*Success, Failure*
Audit logon events	*Success, Failure*

Audit policy	Setari minimale recomandate
Audit object access	*la latitudinea administratorului, in funcţie de modelul de securitate ales*
Audit policy change	*Success*
Audit privilege use	*No auditing (eventual)*
Audit process tracking	*No auditing*
Audit system events	*Success*

✓ **Serverul DNS**

- dacă este posibil, se recomandă folosirea modelului de server DNS cu baza de date a serviciului integrată în *Active Directory*
- este necesară de multe ori dezactivarea *dynamic update* sau folosirea *dynamic update secure*
- se recomandă restricţionarea transferului de zone
- este utilă activarea setării ***Secure cache against pollution*****,** pentru a împiedica preluarea de date eronate (de obicei in mod intenţionat) din *cache*-ul altor servere
- este recomandată redimensionarea jurnalelor DNS (*log*), recomandat 16 MB

✓ **Serverul DHCP**

- se vor monitoriza încercarea şi introducerea în reţea a unui nou server DHCP, neautorizat
- se recomandă restricţionarea accesului la jurnalele (*log*) DHCP
- este necesară de cele mai multe ori creşterea dimensiunii jurnalelor DHCP
- se vor restrânge drepturile administrative la serverul DHCP, ce vor fi acordate numai persoanelor autorizate să administreze şi / sau să opereze asupra serverului DHCP

✓ **Serverul WINS**

- Se recomandă restricţionarea accesului la serverul WINS; vor avea acces la server numai utilizatorii cu drept de administrare
- în cazul în care se foloseşte procedura de replicare între serverele WINS, se recomandă monitorizarea replicării datelor între servere WINS

- se recomandă activarea jurnalizării (*logging*) WINS
- de cele mai multe ori se recomandă folosirea intrărilor statice – controlate strict – în baza de date WINS, în locul înregistrărilor dinamice

✓ **Serverul de fişiere**

- vor fi strict configurate permisiunile NTFS şi a cele de partajare
- se recomandă utilizarea şi configurarea exemplarelor „*shadow*”

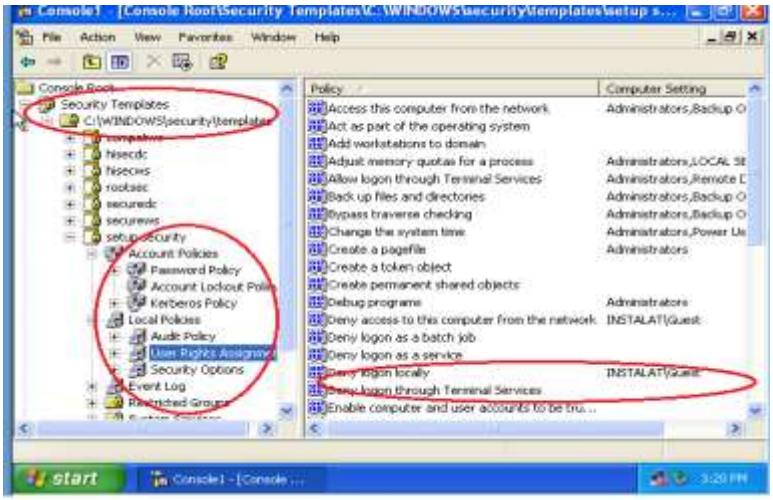
Machete de securitate

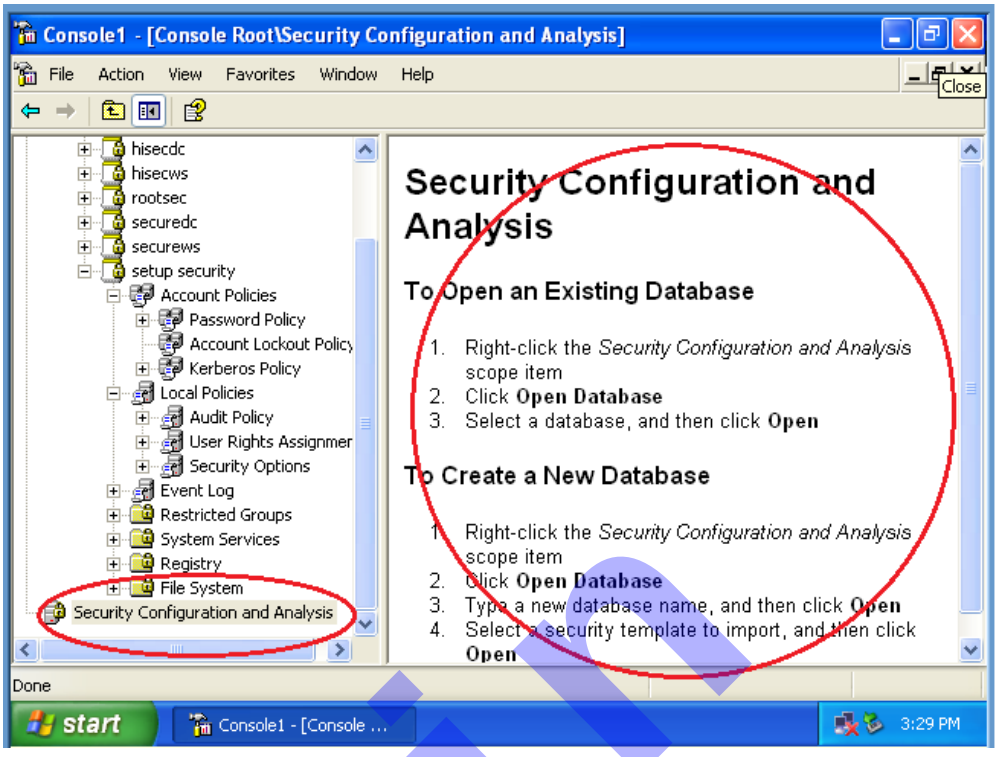
Securitatea unei reţele nu este completă dacă nu este rezolvată şi securitatea calculatoarelor client, calculatoare cunoscute şi sub numele de staţii de lucru.

Cele mai răspândite metode pentru asigurarea şi urmărirea funcţionării regulilor de securitate pentru calculatoarele din reţea sunt următoarele:

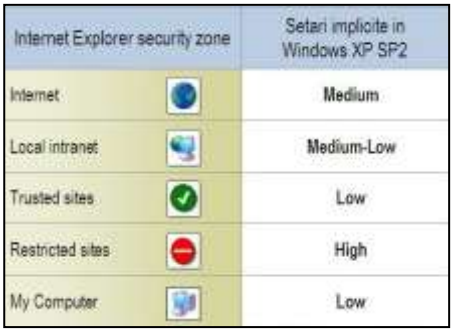
Template	Descriere
Enterprise client	Enterprise Client – Desktop.inf Enterprise Client – Laptop.inf
High security	High Security – Desktop.inf High Security – Laptop.inf
Stand-alone	Legacy Enterprise Account.inf Legacy Enterprise Client – Desktop.inf Legacy Enterprise Client – Laptop.inf Legacy High Security Account.inf Legacy High Security – Desktop.inf Legacy High Security – Laptop.inf
	Legacy High Security Account.inf Legacy High Security – Desktop.inf Legacy High Security – Laptop.inf

- aplicarea machetelor de securitate (*security template*); machetele de securitate sunt fişiere cu extensia .inf care pot fi utilizate prin componenta *Security Templates* a consolei *mmc.*

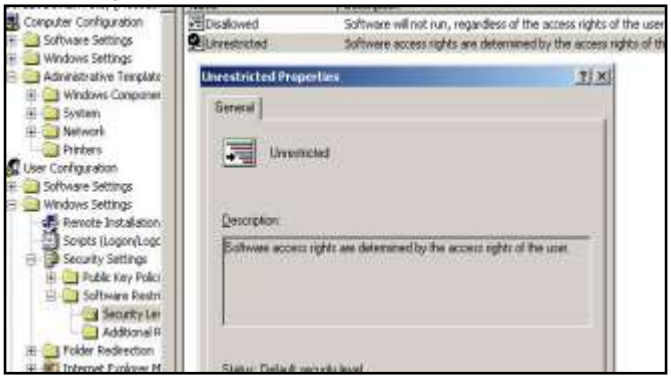




- utilizarea sistemului de fişiere NTFS
- redimensionarea jurnalelor pentru evenimente
- supravegherea accesului prin proceduri de audit
- configurarea corectă a *browser*-ului *Internet Explorer* şi a oricărui alt *browser*.



- utilizarea – ori de câte ori este posibil – a machetelor .adm, ca de ex. cele furnizate de *Office Resource Kit,* în vederea implementării unor reguli de securitate specifice aplicaţiilor sau pachetelor de aplicaţii
- protejarea accesului prin proceduri şi componente de tip *Windows firewall*
- implementarea politicilor restrictive – inclusiv cele legate de restricţii software faţă de utilizarea anumitor aplicaţii instalate - folosind obiecte GPO (*Group Policy Object*)



WSUS (Windows Server Update Services)

WSUS este instrumentul folosit pentru gestionarea şi distribuirea actualizărilor aduse sistemelor de operare şi aplicaţiilor, în vederea rezolvării vulnerabilităţilor legate de securitate şi a problemelor de stabilitate.

În mod tradiţional, administratorii accesează frecvent *site*-urile Microsoft pentru găsirea actualizărilor (corecţiilor) potrivite. De obicei le descarcă manual, le testează şi, dacă se potrivesc mediului de operare, le distribuie pe calculatoarele care au nevoie de ele, făcând o actualizare „manuală" a componentelor.

Microsoft Update este un *site Web* folosit pentru actualizarea componentelor software: sisteme de operare, aplicaţii, drivere, alte componente - legate de securitate şi stabilitate. *Site*-ul este permanent actualizat (el însuşi) oferind cele mai noi actualizări şi corecţii pentru sistemele de operare din familia Microsoft.

Actualizările (corecţiile) sistemelor de operare pot fi:

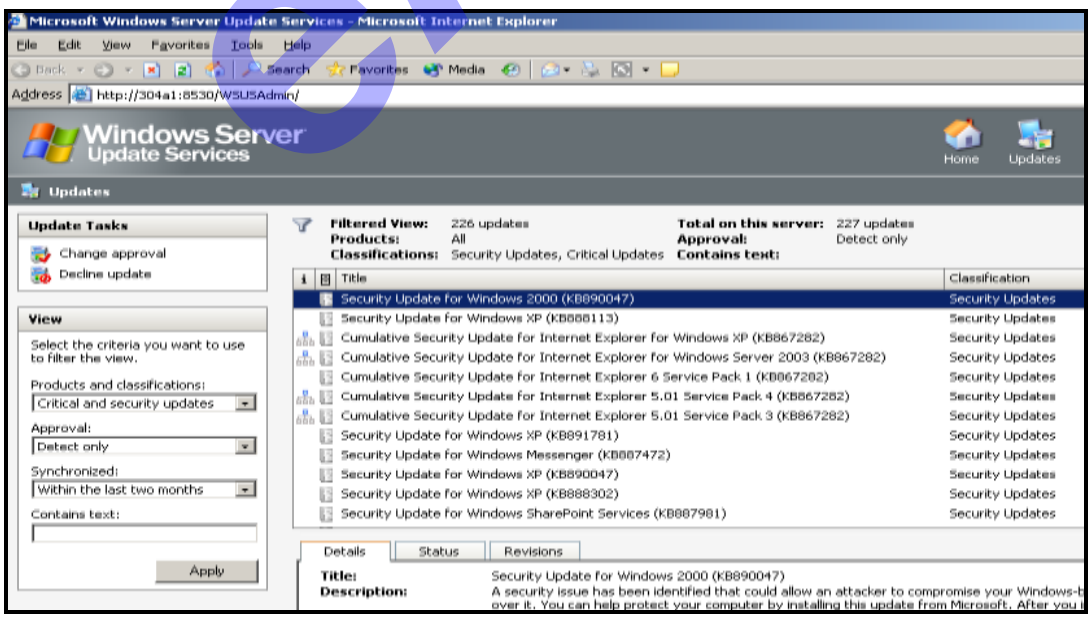
- actualizări **critice**: corecţii de securitate şi alte actualizări importante, legate mai ales de securitatea calculatoarelor şi a reţelelor
- recomandări: fişiere a căror descărcare este recomandată, de obicei componente de tip „*service pack*"
- instrumente**:** utilitare de interes
- actualizări **pentru Internet şi multimedia:** ultimele modificări aduse componentelor *Internet Explorer, Windows Media Player*; etc.
- componente **adiţionale:** caracteristici pentru *desktop* şi componente ale sistemelor de operare în general
- **caracteristici multilingvistice:** meniuri, cutii de dialog, suport pentru lucrul în altă limbă decât engleza
- ghiduri **de utilizare şi de instalare**

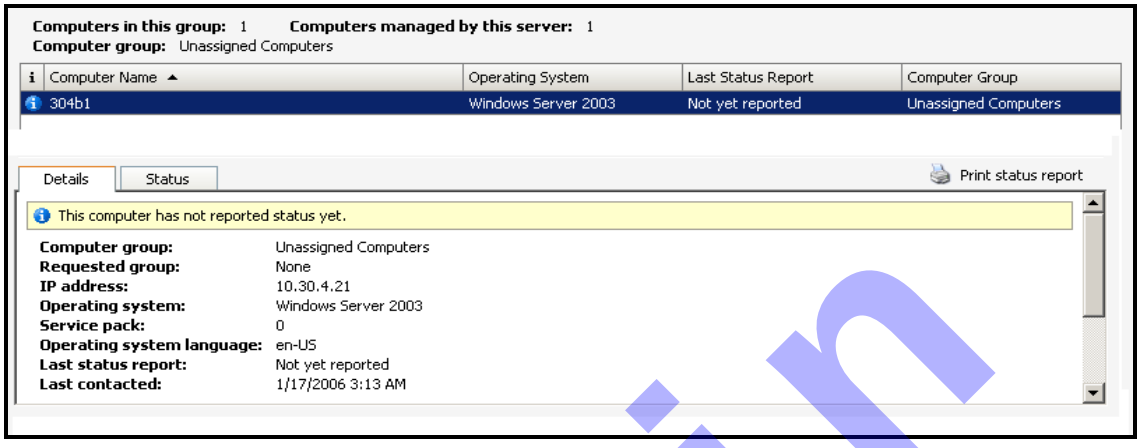
Actualizarea automată este o caracteristică configurabilă a sistemelor de operare Windows, prin care se instalează şi configurează componente sistem, fără intervenţia utilizatorului. Actualizările provin din descărcarea automată a unor fişiere de la *Microsoft Update Web* sau de la un server WSUS. Configurarea actualizării automate este controlată în mod centralizat de către Administrator.

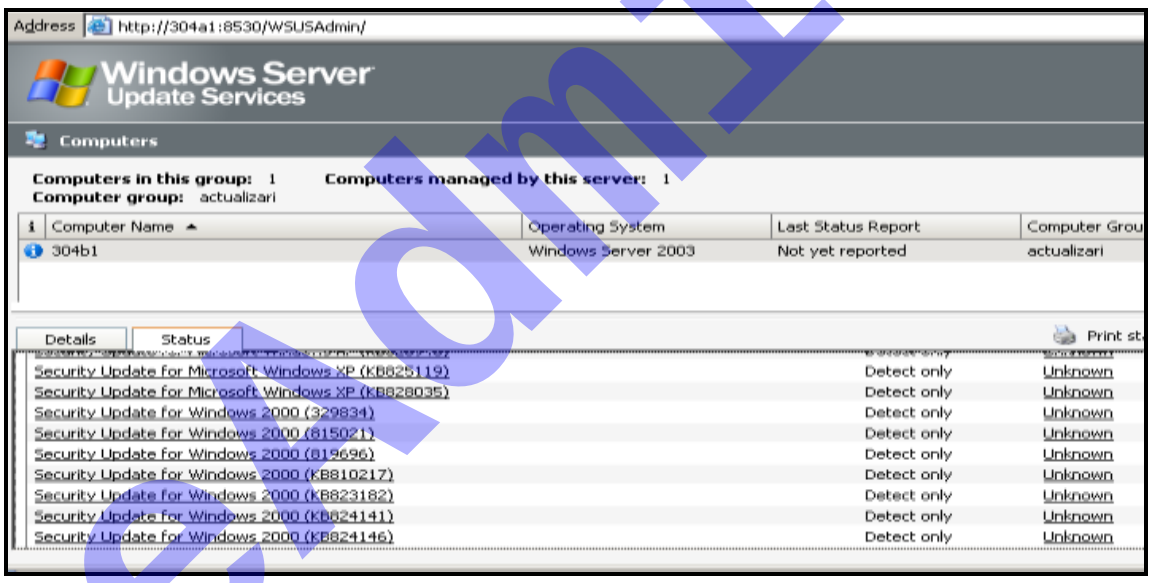
Instalarea componentelor actualizate şi a corecturilor poate avea loc:

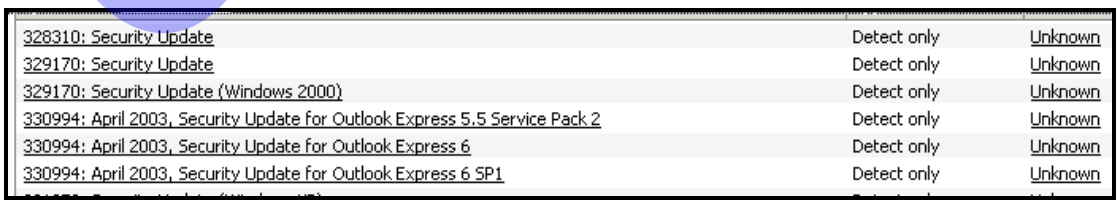
- „automat”: componentele sunt descărcate automat şi instalate la un moment de timp programat. Acesta este modul de lucru recomandat pentru că operează modificări valabile pentru toţi utilizatorii.
- „descărcare automată – instalare la cerere”: actualizările se descarcă automat dar nu sunt instalate decât la cererea administratorului.
- „notificare”: actualizările nu sunt nici descărcate nici instalate automat. Administratorii (cu sesiuni locale deschise la respectivul server) primesc notificări referitoare la componentele care admit actualizări şi la posibilitatea descărcării şi instalării lor.
- „anularea actualizării automate”: nu apar notificări despre actualizări şi corecţii.

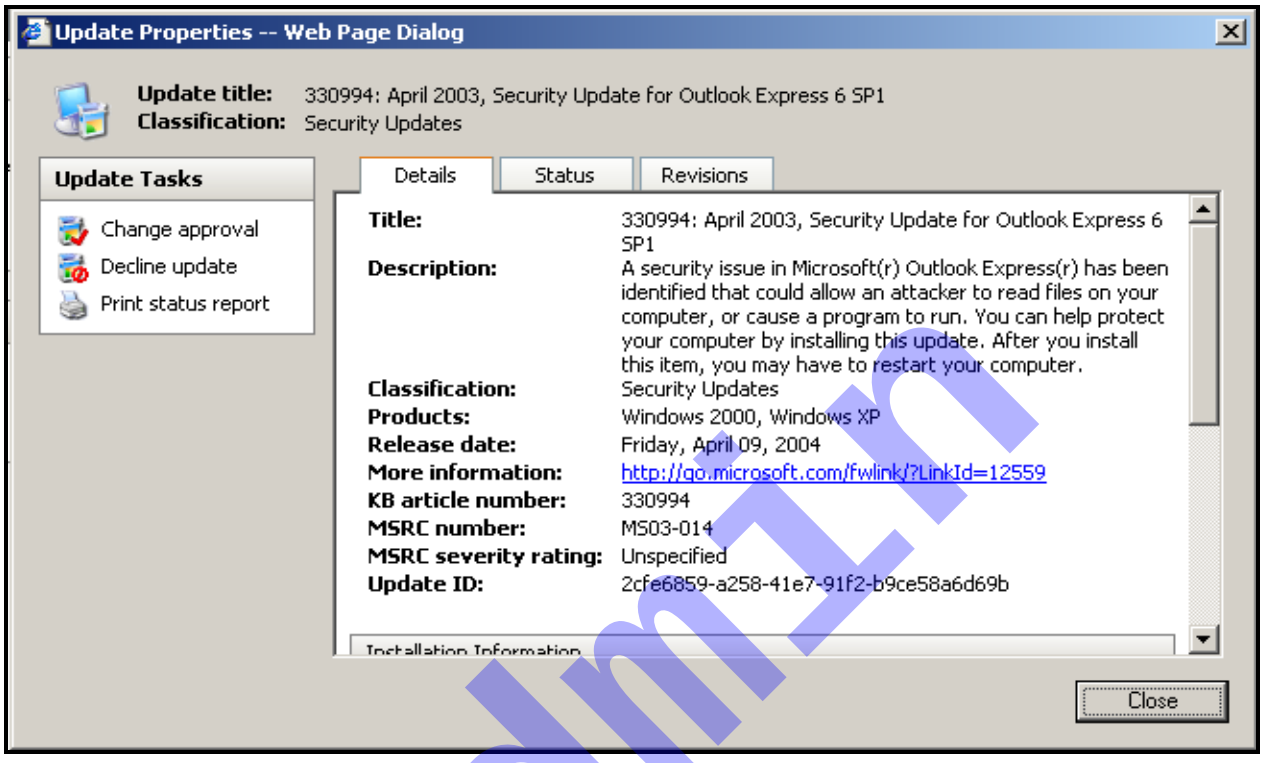
WSUS (***Windows Server Update Service***) este o componentă opţională pentru sistemele de operare Windows Server 2003. Serviciul poate fi descărcat de pe *site*-ul *Web* al Microsoft. Va acţiona ca un punct central al reţelei, folosit pentru distribuirea actualizărilor necesare calculatoarelor client şi serverelor. WSUS poate oferi servicii de actualizare pentru: sisteme de operare, pentru Microsoft Office, Exchange Server, SQL Server. WSUS va fi instalat pe un server din reţea şi va fi configurat astfel încât să-şi sincronizeze conţinutul cu cel al *site*-ul Microsoft *Update Web*, ori de câte ori actualizările sunt disponibile. Sincronizarea se face automat sau manual ce către administrator.

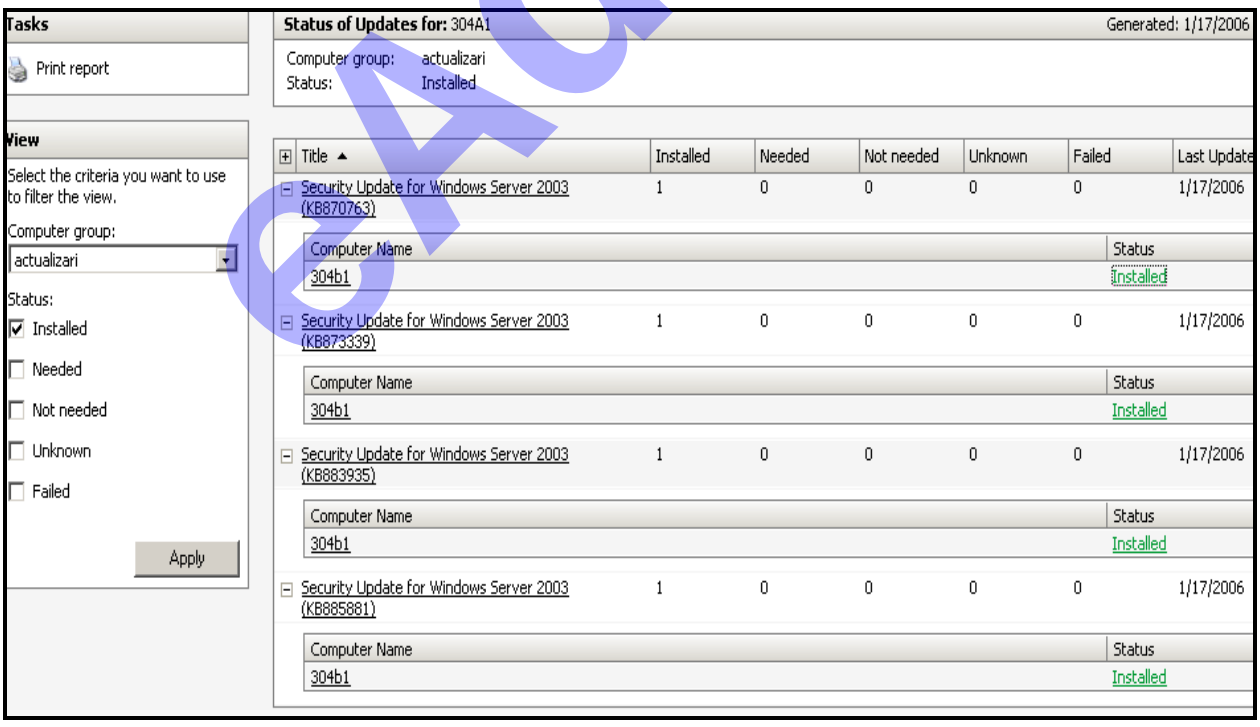



Computers in this group: 1
Computers managed by this server: 1
Computer group: Unassigned Computers
Computer Name
Operating System
Last Status Report
Computer Group
304b1
Windows Server 2003
Not yet reported
Unassigned Computers
Details
Status
Print status report
This computer has not reported status yet.
Computer group: Unassigned Computers
Requested group: None
IP address: 10.30.4.21
Operating system: Windows Server 2003
Service pack: 0
Operating system language: en-US
Last status report: Not yet reported
Last contacted: 1/17/2006 3:13 AM


Address
http://304a1:8530/WSUSAdmin/
Windows Server
Update Services
Computers
Computers in this group: 1
Computers managed by this server: 1
Computer group: actualizari
Computer Name
Operating System
Last Status Report
Computer Grou
304b1
Windows Server 2003
Not yet reported
actualizari
Details
Status
Print st
Security Update for Microsoft Windows XP (KB825119)
Security Update for Microsoft Windows XP (KB828035)
Security Update for Windows 2000 (329834)
Security Update for Windows 2000 (815021)
Security Update for Windows 2000 (819696)
Security Update for Windows 2000 (KB810217)
Security Update for Windows 2000 (KB823182)
Security Update for Windows 2000 (KB824141)
Security Update for Windows 2000 (KB824146)
Detect only
Unknown


328310: Security Update
329170: Security Update
329170: Security Update (Windows 2000)
330994: April 2003, Security Update for Outlook Express 5.5 Service Pack 2
330994: April 2003, Security Update for Outlook Express 6
330994: April 2003, Security Update for Outlook Express 6 SP1
Detect only
Unknown

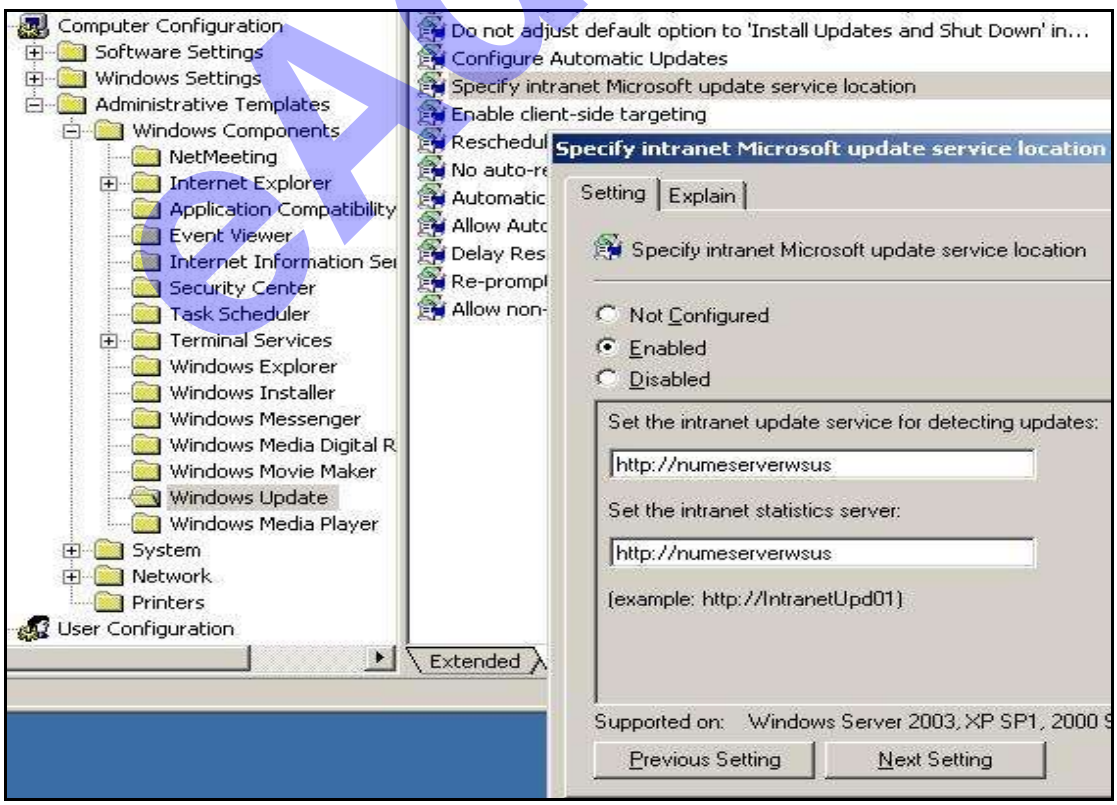

Update Properties -- Web Page Dialog
Update title: 330994: April 2003, Security Update for Outlook Express 6 SP1
Classification: Security Updates
Update Tasks
Change approval
Decline update
Print status report
Details
Status
Revisions
Title: 330994: April 2003, Security Update for Outlook Express 6 SP1
Description: A security issue in Microsoft(r) Outlook Express(r) has been identified that could allow an attacker to read files on your computer, or cause a program to run. You can help protect your computer by installing this update. After you install this item, you may have to restart your computer.
Classification: Security Updates
Products: Windows 2000, Windows XP
Release date: Friday, April 09, 2004
More information: http://go.microsoft.com/fwlink/?LinkId=12559
KB article number: 330994
MSRC number: MS03-014
MSRC severity rating: Unspecified
Update ID: 2cfe6859-a258-41e7-91f2-b9ce58a6d69b
Close


Tasks
Print report
View
Select the criteria you want to use to filter the view.
Computer group:
actualizari
Status:
Installed
Needed
Not needed
Unknown
Failed
Apply
Status of Updates for: 304A1
Generated: 1/17/2006
Computer group: actualizari
Status: Installed
Title
Installed
Needed
Not needed
Unknown
Failed
Last Update
Security Update for Windows Server 2003 (KB870763) 1 0 0 0 0 1/17/2006
Computer Name
Status
304b1
Installed
Security Update for Windows Server 2003 (KB873339) 1 0 0 0 0 1/17/2006
Computer Name
Status
304b1
Installed
Security Update for Windows Server 2003 (KB883935) 1 0 0 0 0 1/17/2006
Computer Name
Status
304b1
Installed
Security Update for Windows Server 2003 (KB885881) 1 0 0 0 0 1/17/2006
Computer Name
Status
304b1
Installed

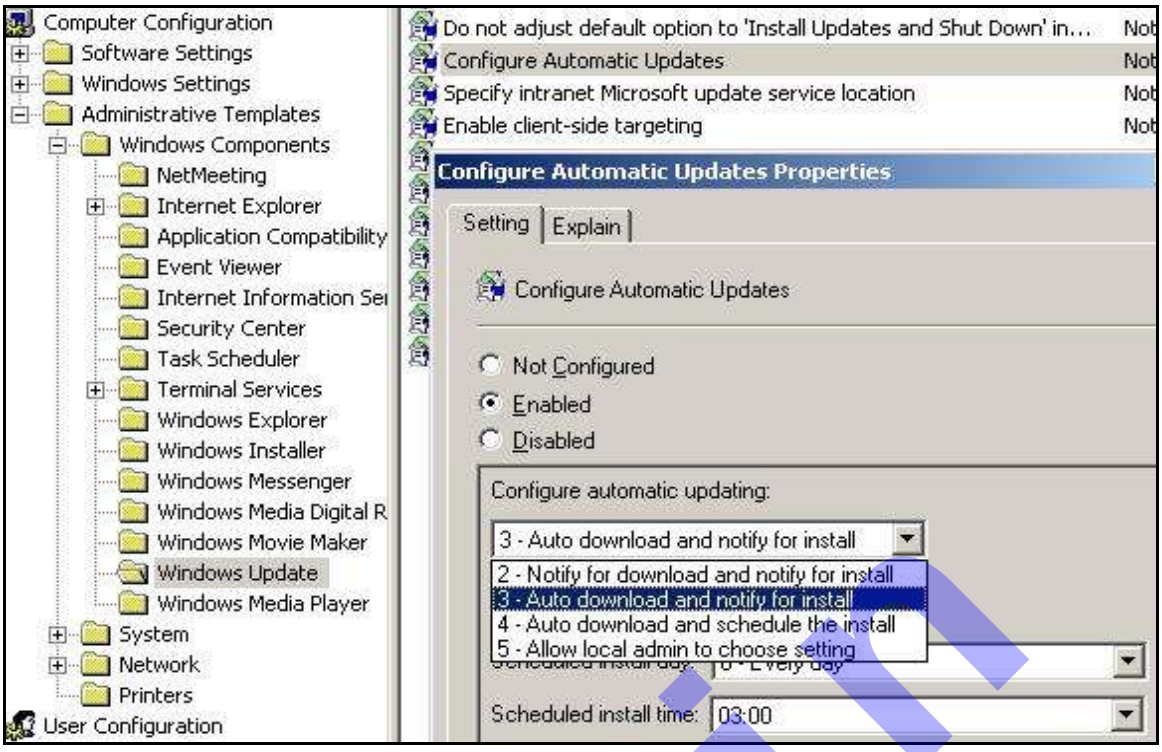
Computer Name	Installed	Needed	Not needed	Unknown	Failed	Last Update
304b1	4	32	210	11	0	1/17/2006

Update Title	Approval	Status
823559: Security Update for Microsoft Windows	Detect only	Needed
Critical Update for Windows Media Player Script Commands (KB828026)	Detect only	Needed
Cumulative Security Update for Internet Explorer for Windows Server 2003 (KB824145)	Detect only	Needed
Cumulative Security Update for Internet Explorer for Windows Server 2003 (KB834707)	Detect only	Needed
Cumulative Security Update for Internet Explorer for Windows Server 2003 (KB867282)	Detect only	Needed
Cumulative Security Update for Internet Explorer for Windows Server 2003 (KB867801)	Detect only	Needed
Cumulative Security Update for Outlook Express for Windows Server 2003 (KB823353)	Detect only	Needed
Flaw In Windows Media Player May Allow Media Library Access (819639)	Detect only	Needed
MS03-026: Security Update for Windows Server 2003 (823980)	Detect only	Needed
October 2003, Cumulative Patch for Internet Explorer for Windows Server 2003 (KB828750)	Detect only	Needed
Security Update for Microsoft Windows (KB824105)	Detect only	Needed
Security Update for Microsoft Windows (KB824141)	Detect only	Needed
Security Update for Microsoft Windows Server 2003 (KB825119)	Detect only	Needed
Security Update for Microsoft Windows Server 2003 (KB828035)	Detect only	Needed

WSUS este versiunea server pentru *Microsoft Update* care poate rula intr-o reţea locală şi care permite centralizarea instalării de actualizări software intr-o organizaţie: vor fi instalate numai anumite actualizări, cele aprobate de către un administrator. Serverul WSUS contactează *Microsoft Update* pentru a obţine lista de *update*-uri existente şi eventual necesare. Clienţii folosesc *Automatic Updates Client* cu ajutorul căruia se conectează la serverul WSUS, de unde vor fi preluate actualizările. Fiecare computer poate fi plasat intr-un grup de computere şi pot fi aprobate *update*-uri diferite pentru fiecare grup in parte.



Specificarea serverului WSUS ce va fi folosit de către clienţi se face cu ajutorul obiectelor GPO.



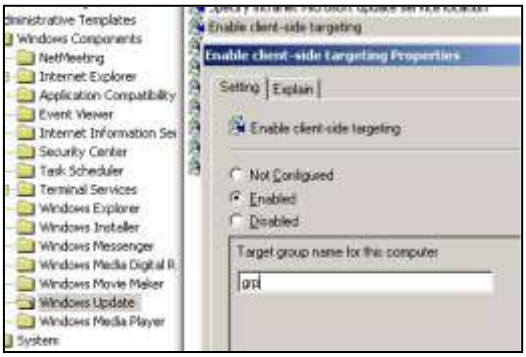
După instalare, serverului WSUS se va sincroniza cu *Microsoft Update*. Sincronizarea se se va face manual sau automat, la anumite intervale de timp definite de administrator. *Update*-urile ce vor ajunge la clienţi trebuie aprobate de către administrator. Marcajele care indică tipul de aprobare sunt:

Install – realizează instalarea

Detect Only - nu face instalare ci sunt doar detectate, căutate, componentele care ar avea nevoie de un *update*

Remove – pentru dezinstalarea anumite *update*-uri , de ex cele care in urma instalării au produs probleme

Decline – nu se va face instalarea acelui update



Calculatoarele din reţea fac parte în mod automat din grupurile *All Computers* şi *Unassigned Computers.* Un computer poate fi scos însă din acest ultim grup şi introdus in altul.

Pentru fiecare grup de computere se pot stabili politici diferite de aprobare a *update*-ului.

Adăugarea la un grup de computere se poate face fie specificând acest lucru folosind un GPO, fie adăugând manual din interfaţa WSUS fiecare client în grupul dorit.

Propunere de temă practică

1. Identificaţi ameninţările specifice reţelei dvs. Ajutaţi-vă de orice diagramă, desen, tabel care descrie reţeaua de calculatoare, amplasarea calculatoarelor şi a echipamentelor de comunicaţii în reţea, modul de lucru în general. Evaluaţi probabilitatea de materializare a fiecărei ameninţări, impactul sau paguba suferită. Paguba poate fi la fel de importantă şi în situaţia unei pierderi materiale dar şi a pierderii de imagine, de credibilitate.

   Completaţi tabelul ameninţărilor identificate şi a vulnerabilităţilor care pot fi speculate, fie din interior fie din exterior.

Exemplu:

Ameninţare	**Vulnerabilităţi**	**Probabilitatea de materializare**	**Impact, pierdere, pagubă** (Evaluare 1 ….10)	**Rang, prioritate** (Probabilitatea *Paguba)
Expunerea şi folosirea improprie a datelor cu caracter secret, confidenţial, sau de altă natură *Se regăsesc aici toate elementele STRIDE*	**Acces neautorizat la baza de date**	0,7	9	0,63
	Parola administratorului este cunoscută de multă lume			
	Acces fizic la serverul cu baza de date unde este permanent deschisă o sesiune de administrator			
	Server nesupravegheat, incinta cu acces aproape liber			
	Atac din exterior prin Internet			

	Utilizatori neautorizaţi au acces la date			
Periclitarea funcţionării serverului Web *Se regăsesc aici elementele STR DE* *Informaţiile sunt publice deci nu sunt expuse neautorizat.*	**Oprirea / blocarea serviciului, alterarea informaţiilor** ***(atac din exterior sau din interior)***	mică	de imagine	? *(va fi evaluată ulterior)*
	Serverul *Web* nu se află într-o reţea protejată (DMZ, perimetru, *firewall*)			
	Accesul la pagina / paginile *Web* este public (fără autentificare)			

2. Revizuiţi tabelul ameninţărilor şi vulnerabilităţilor. Identificaţi pentru fiecare vulnerabilitate o soluţie de rezolvare: de eliminare cu totul a vulnerabilităţii sau măcar de diminuare a pierderilor, a pagubelor.
3. Ordonaţi vulnerabilităţile după importanţă, după rang. Veţi obţine o primă formă a strategiei de securitate care ar putea fi implementată, dacă vă îndreptaţi atenţia asupra soluţiilor, acţiunilor, operaţiilor care trebuie întreprinse pentru diminuarea sau eliminarea pagubelor, respectiv reducerea vulnerabilităţilor. Vulnerabilităţile pot fi tratate acum drept riscuri. Managementul riscului se va referi de aici încolo la: care dintre riscuri (vulnerabilităţi) sunt mai importante decât altele, ce riscuri trebuie rezolvate mai întâi, ce riscuri vor fi analizate mai târziu, care sunt costurile aplicării măsurilor de securitate pe care le-aţi stabilit.
4. Revizuiţi tabelul ameninţărilor / vulnerabilităţilor / riscurilor. Verificaţi dacă soluţiile de securitate pe care le-aţi construit respectă cerinţele teoretice şi practice ale securităţii reţelelor:
   - ✓ Apărarea în profunzime: reţea, calculator, aplicaţie, date

- ✓ Regulile, măsurile de securitate sunt aplicate: administrativ, software, fizic
- ✓ Privilegiul minim: utilizatorii dispun de minimul necesar şi suficient de privilegii pentru rezolvarea sarcinilor
- ✓ Suprafaţa de atac din exterior (Internet) este minimă
- ✓ Riscurile: acceptate, atenuate, transferate, eliminate

Revizuiţi în consecinţă tabelul ameninţărilor /vulnerabilităţilor / riscurilor şi completaţi pe de o parte ameninţări / vulnerabilităţi şi pe de altă parte acţiuni / măsuri de eliminare sau diminuare a pagubelor.

5. Construiţi un plan de acţiune pentru situaţia în care apare un incident de securitate. Pentru cunoaşterea mai bună a condiţiilor şi contextului în care a apărut incidentul trebuie să fie pregătite din vreme jurnale de evenimente şi poate alte proceduri de audit. Folosiţi şi un registru (jurnal) în care să fie înscrise incidentele de securitate care au avut loc. Orice revizuire ulterioară a tabelului cu vulnerabilităţi va porni de la incidentele, evenimentele semnalate şi înscrise în jurnal.

Ce aţi învăţat în acest modul?

- ✓ să identificaţi şi să evaluaţi ameninţări, vulnerabilităţi şi riscuri
- ✓ să analizaţi riscuri şi să evaluaţi pagubele
- ✓ să evaluaţi gradul de securitate a unei reţele şi a fiecărei componente în parte
- ✓ să concepeţi măsurile de securitate cele mai potrivite pentru asigurarea securităţii unei reţele
- ✓ să construiţi – şi la nevoie – să impuneţi reguli de securitate pentru reţeaua pe care o administraţi
- ✓ să creşteţi gradul de securitate a reţelei pe care o administraţi
- ✓ să construiţi un plan de acţiune pentru situaţia în care apar şi sunt detectate incidente de securitate