Bezpečnost dat v lokálních počítačových sítích, síťový operační software Netware od společnosti Novell

Magdalena Chmelařová[a], Jiří Schindler[b],

[a] Filosoficko-přírodovědecká fakulta, Slezská univerzita v Opavě, Bezručovo náměstí 13, Opava 746 01, Česká republika

[b] Fakulta ekonomická, VŠB – Technická univerzita Ostrava, Sokolská 33, 701 21 Ostrava1, Česká republika

Abstrakt

Každá organizace, která má počítačovou síť, by měla mít svoji specifickou bezpečnostní politiku. Na její tvorbě se musí podílet hlavně vedoucí pracovníci, profesionálové z oblasti informatiky, ale i obyčejní uživatelé. Hlavním úkolem je určit, co se má chránit a pak určit, jak zajistit bezpečný provoz sítě.

Bezpečnost by měla zaručit: „*dostupnost*“ - prvky sítě, informace a služby jsou kdykoliv dostupné v případě potřeby, „*důvěryhodnost*“ - služby a informace jsou dostupné pouze oprávněným uživatelům podle daných privilegií, „*integrita*“ - komponenty a informace nejsou zničeny, porušeny nebo zcizeny. Bezpečnost sítě může být ohrožena nebo narušena s ohledem na technickému vybavení, programovému vybavení, informacím či dokonce k síťovým operacím. V této práci se zaměříme na zabezpečení v lokálních počítačových sítích a na možnosti síťového operačního systému Netware.

Zabezpečení sítě obecně

Ohrožení hardwaru (*Threads to Hardware*) - zde patří veškeré technické vybavení sítě, objekty typu počítače, periferie, kabely, telekomunikační linky, obvody či jakákoliv jiná technická zařízení připojená k síti. Každý z těchto objektů může být ohrožen poškozením či zničením. Rozsah možnosti ohrožení hardwaru je téměř neomezený (krádež, přerušení kabelů, fyzické zničení zařízení, neoprávněné zapojení komponent atd.). Tady je nutná pravidelná technická kontrola všech objektů v síti, fyzické zabezpečení hardwaru proti krádeži, používání ochranných jističů a dalších zabezpečovacích zařízení.

Ohrožení softwaru (*Threads to Software*) - zde se řadí veškeré programové vybavení pracovních stanic a serverů. Jsou to operační systémy, aplikace a jiné programy nutné pro provoz sítě. Data budeme řadit do jiné oblasti. Softwaru hrozí následující: „*Smazání*, *krádež, napadnutí virem, trojským koněm nebo parazitem*, mohou mu hrozit skryté chyby (*štěnice – bug*), které se projevují po určitém běhu programu a za určitých okolností“. Síťové správní programy mohou umožnit sledování pokusů o smazání nebo poškození programů, antivirové programy mohou zabezpečit software proti virům.

Ohrožení informací (*Threads to Information*) - v této souvislosti informace značí konfigurace, soubory, přenosy a další reprezentace dat. K ohrožení může patřit: „*Úmyslné smazání databáze, krádež, ztráta dat během havárie sítě, poškození dat*“. Některé druhy poškození informací mohou být odhaleny pomocí cyklických nadbytečných kódů nebo dalších metod detekce chyb. Pokusy o smazání datových souborů mohou být detekovány některými řídícími nebo antivirovými programy.

Ohrožení síťových operací (*Threads to Network Operation*) zahrnuje činnosti běžné pro provoz sítě, jako jsou přenosy dat a monitorování a řízení sítě. Ohrozit síťové operace může přerušení kabelového spojení nebo zhavarování uzlů na síti. Interference zahrnuje elektrické šumy, nebezpečím je rovněž přetížení sítě, kdy může dojít ke ztrátám nebo poškození paketů. Sítě, jejichž data jsou přenášena pomocí optických kabelů, jsou méně náchylné k interferencím a přetížením.

Úrovně zabezpečení (*Security Levels*) jsou v publikacích vydávaných vládou USA definovány jako čtyři universální třídy zabezpečení (*třída D* - minimální bezpečnost - systémy v této třídě nejsou bezpečné, *třída C* - volitelné řízení přístupu - operační systémy jako UNIX nebo jakýkoliv síťový operační systém poskytují heslovou ochranu nebo přístupová práva, lze sledovat a zaznamenávat všechny činnosti uživatelů, zabránit nepovoleným uživatelům k využívání sítě, přístupu k datům apod., *třída B* - povinné řízení přístupu - tyto systémy mohou obecně být schopny poskytovat matematickou dokumentaci bezpečnosti, sledování pokusu o porušení bezpečnosti a udržování bezpečnosti i v případě selhání systému, *třída A* - ověřená ochrana - systémy této třídy musí matematicky ověřit, že jejich bezpečnostní systém splňuje specifikace a požadavky na bezpečný systém).

Bezpečnostní otázky v sítích Netware

Netware je síťový operační systém pro správu a obsluhu lokálních počítačových sítí od společnosti Novell. V současné době je používáno několik verzí Netware. V článku ochrana dat poukazujeme na možnosti ochrany dat ve verzi 4.x. Od této verze je ochrana rozdělena na NDS ochranu a na ochranu souborového systému. Jaké možnosti má správce neboli administrátor sítě?

První možností, jak zajistit bezpečný přístup do sítě a správné využívání dat, je využít správu NDS (*Netware Directory Services*). Je to globální jmenná služba (*distribuovaná databáze*), která umožňuje při vytváření bezpečnostní politiky přesně definovat, kdo smí používat systém a jeho služby. Tato služba je organizována jako strom a obsahuje informace o uživatelích, uzlech a technickém

vybavení sítě, dále o logických objektech jako jsou skupiny a o objektech, které pomáhají organizovat jiné objekty. Práva objektů (*object rights*) se vztahují k objektům v globální databázi NDS. Jsou definována následující práva:

- „Supervizor“ – poskytuje všechna přístupová práva k objektu.
- „Browse“ – poskytuje právo pro přístup k objektu stromu.
- „Create“ – poskytuje práva vytvářet objekt pod jiným objektem.
- „Delete“ – poskytuje právo smazat objekt ze stromu.
- „Rename“ – poskytuje právo měnit jméno objektu.

Práva mohou být přiřazena nebo zděděna z objektu nad ním. Práva vlastností (*property rights*) se vztahují k vlastnostem objektu v NDS. Kvůli organizačním hlediskům je rozdělena NDS do sekcí (*sekci tvoří skupina příbuzných objektů*). Toto seskupení je pak použito jako základ pro vytváření replik každé sekce. Repliku tvoří jednoduchá kopie sekce a zaručuje, že se sníží poruchovost a zvýší odolnost proti chybám.

Druhá možnost ošetření je využívání „File system security“ - je to struktura, která se používá pro záznamy o souborech. Systém souborů má tři hlavní úrovně:

- Svazek (*volume*), což je nejvyšší úroveň a označuje partition, vytvořenou instalačním programem.
- Adresář (*directory*), což je střední úroveň, která obsahuje další adresáře nebo soubory.
- Soubor, což je nejkonkrétnější úroveň. Toto je úroveň, na které pracují uživatelé nebo procesy.

Správce sítě může vytvořit účet uživateli nebo celé skupině uživatelů, kteří sdílejí jisté bezpečnostní charakteristiky. První bezpečnost je na úrovni přihlášení, kdy každý přístup do sítě je kontrolován přihlašovacím skriptem. Kdo a jak se může přihlásit, zajišťuje „Login security“. Každý uživatel musí zadat jméno a heslo přístupu do sítě. Jakým způsobem je zajištěna bezpečnost? V případě, že bude zadáno špatné jméno nebo heslo, není povolen přístup do sítě. Zjišťování vetřelců (*anglicky intruder detection*) je způsob, kterým Netware rozeznává pokusy o přihlášení s chybně zadaným heslem. Supervisor může nastavit tento počet v rozmezí od 1 až do 7 chybných přihlášení potřebných k uzamčení účtu. Rovněž je k dispozici i délka intervalu (*10 minut až 7 dní*). Tuto volbu nastavíme pomocí Netware Administrator. Můžeme rovněž uživatelům nastavit, aby pravidelně měnili svá hesla. Musíme nastavit, aby po určitém počtu chybných přihlášení byly uživatelské účty zamčené. Jak to zajistit, ukazuje tabulka:

Tabulka 1: *Nastavení pro zjišťování nepovoleného přihlášení*

Volba	Nastavení
Detect Intruder	ano (umožňujeme proces sledování)
Intruder Detection Threshhold	x
Incorrect Login Attempts	x (počet chybných přihlášení)
Lock Account After Detection	ano (dojde k uzamčení)
Length Account Lockout	x *dnů* x *hodin* x *minut* (co nejdelší)
Bad Login Retention Time	x *dnů* x *hodin* x *minut*

Po úspěšném přihlášení je uživatelům povolena práce v síti v rámci pozice v NDS a v rámci souborového systému (*File system security*). Poté, co se uživatelé připojí k nějakému souborovému serveru, provede se jeho systémový skript. Netware používá přihlašovací předpis pro připojení k dalším serverům, mapování uživatelových specifických mechanik a provádění dalších funkcí. Po jeho provedení se spustí skript konkrétního uživatele. Netware ukládá například uživatelské přihlašovací skripty do adresáře SYS:MAIL.

Co je to udělení pověření? Udělení pověření (*trustee assignment*) je přístupová řídicí funkce, kterou Netware používá pro to, aby nějaké uživatelské identifikaci dovolil provádět specifický přístup k nějakému adresáři, podadresáři nebo souboru. Nesmíme zapomenout, že je-li pověření přiřazeno na úrovni adresáře, platí pro všechny podadresáře a jejich soubory. Netware spojuje dohromady práva přiřazená uživatelově individuální identifikaci a určuje uživatelova přístupová práva k adresáři nebo souboru, ke kterému se pokouší o přístup.
Co je to Inherited Rights Mask? Když uživatel vytváří adresáře nebo soubory, automaticky dojde k chránění pomocí „Inherited Rights Mask“ (*zděděná maska oprávnění*). Tato maska dovoluje, aby uživatelé měli přístupy Read a FileScan . Jestliže supervisor definuje oprávnění pro uživatele, pak tato definovaná oprávnění převáží nad touto maskou.

Tabulka 2: *Práva uživatelů k souborům a adresářům*

Oprávnění	Popis
Supervisor	Veškerá práva pro soubory i adresáře
Read	Čtení souborů v nějakém adresáři a spouštění programů
Write	Čtení a změny souborů
Create	Vytváření souborů a adresářů
Erase	Odstranění adresáře i souborů
Modify	Změna atributů adresáře a souborů
FileScan	Prohlížení
Access Control	Měnit udělená práva

Udělení práv aplikacím umožňuje program „*aprite*“, který spadá do kategorie freeware. Tento program může správce sítě použít pro udělení práv aplikacím a aplikace mohou běžet s právy Netware. Bližší informace lze získat na adrese: http://www.coil.com/~eb-right/aprite.zip.

Tabulka 3: *Jak udělovat práva?*

Požadavek	Jaké práva?
Otevřít a číst soubor	Read
Podívat se na soubor	File Scan
Hledat soubor v adresářích	File Scan
Otevření a zápis do souborů	Write, Create,Erase, Modify, File Scan, Read
Spustit .EXE soubory	Read, File Scan
Vytvoření adresářů	Create
Kopírování souborů z adresáře	Read, File Scan
Kopírování souborů do adresáře	Write, Create, File Scan
Mazání souborů	Erase
Obnova smazaných souborů, adresářů	Read, File Scan – pro soubory, Create
Měnit atributy	Modify
Měnit masku práv	Access Control

Přístupová privilegia udělují specifická přístupová práva k nějakému souboru nebo k adresáři, zatímco přístupová oprávnění udělují specifická přístupová práva k nějakému adresáři a všem jeho podadresářům. Netware omezuje bezpečnostní přístupová práva na nějaký souborový server. Jestliže máme v naší síťové instalaci serverů více, budeme muset vytvořit nové instalace uživatelů na ostatních serverech.

Často ale potřebujeme v síti vytvořit zvláštní uživatele, kteří budou udělovat přístupová práva jiným uživatelům, aniž by měli plná síťová práva, například vedoucí pracovníci. Tito potřebují mít možnost přidávat další účty pro nové uživatele. Nejvhodnější se jeví zřídit identifikaci manažera pracovní skupiny (Workgroup Manager ID, WMID), který by měl veškerá oprávnění získat od správce sítě. Tím se sníží zátěž na správu sítě.

Kromě různých mechanizmů, které Netware poskytuje supervisorovi pro přiřazení přístupových práv k adresářům a souborům nějakému uživateli, lze použít i program filer, který informuje o přístupových právech skupin a uživatelů.

Nedostatky bezpečnosti Netware

Základní obranou proti všem útokům a napadnutí systému je zabezpečení serveru. Nesmíme zapomenout také na to, že i zaměstnanci mohou poškodit data. Zaměstnanci mohou chtít získat přístup k personálním souborům, zkopírovat je nebo jen tak poškodit či zničit. Proto je nutné síť chránit nejen proti napadnutí zvenku, ale i zevnitř.

Fyzické zabezpečení serveru je první ochrana, a to buď uzamčením klíčem nebo přístupem přes speciální elektronické karty. Důležité soubory je nutné uložit mimo počítač. Mezi nejdůležitější soubory patří *startup.ncf, autoexec.ncf*, soubor

NetWare bindery a soubory adresářového systému NDS. Dále je dobré uložit kopie všech systémových přihlašovacích skriptů, kontejnerových skriptů a všech uživatelských nebo jiných skriptů.

Ochrana přihlašovacích skriptů znamená zabezpečit adresář SYS:_NETWARE. Pomocí rconsole lze prohledávat tento adresář. Narozdíl od binárních souborů z NDS může kdokoliv tyto textové soubory editovat pomocí *edit.nlm*. Jestliže se někdo neoprávněně dostane do sítě, pak uvidí přihlašovací skript a může ho editovat. Proti tomuto útoku se lze bránit pouze tím, že neumožníme přístup ke konzole (*ani na dálku*).

Stejně jako je dobré si vytvořit seznam všech důležitých souborů v síti, abychom je mohli bezpečně chránit, je dobré si vytvořit rovněž seznam všech uživatelů a skupin v síti. Výhodné je pro to použít Netware Administrator. Dále je vhodné hledat podezřelé účty s přístupem supervisor jako třeba GUEST nebo PRINTER. Když kontrolujete uživatele je vhodné neustále ověřovat přístupy a pověření v síti.

V rámci Netware je skutečný souborový server znám jako konzola. Stejně jako je dobré fyzicky zabezpečit konzolu, tak je vhodné zajistit, aby síť protokolovala všechny činnosti, které uživatel provádí na konzole. K tomu slouží program *conlog.nlm*. Je to výborný diagnostický nástroj, protože do souboru SYS:ETC\console.log zaznamenává odpovědi systému.

Dále je vhodné zapnout účtování, které nám umožní sledovat každou operaci přihlášení a odhlášení včetně chybových hlášení. Je výhodné se vyhnout účtu supervisora, s výjimkou nejkritičtějších přístupových práv. Pro přenos paketů je použita metoda, která umožňuje odposlouchávání jakékoliv stanice v síti. Abychom takovému odposlouchávání zabránili, pak musíme požadovat podepisování paketů. Musíme ale přidat do souboru *autoexec.ncf* tento řádek:

SET NCP PACKET SIGNATURE OPTION=3

Tímto síť přinutíme, aby podpisy paketů používala pro každý přenos. Co jsou podpisy paketů? Pro bezpečnou komunikaci se servery Novell používá bezpečnostní praktiku zvanou NCP packet signatures. Obsahuje čtyři úrovně bezpečnosti.

Tabulka 4: *Úrovně podepisování paketů*

Úroveň	Podpis
0	pakety nepodepisují ani server ani klienti
1	podpis - pokud přijímající účastník vyžaduje, aby vysílající podepsal
2	oba účastníci podepisují, pokud nepožaduje - není nutné
3	oba účastníci komunikace podepisují vždy

Podpisy jsou vlastně digitální podpisy připojované ke každému paketu, který uživatel nebo server posílá. Lze obejít podepisování paketů? Pouze tehdy, když není nastavena úroveň zabezpečení 3.

Jak už jsme napsali, program rconsole používejte výjimečně. Tento pomocný program umožňuje supervisorovi sledovat síť na úrovni serveru, aniž by musel u serveru fyzicky být. Pro přihlášení rconsole musí supervisor zadat heslo. Zašifrované heslo se pohybuje po síti a je vystaveno odposlouchávání. Horší situace nastane, když se někdo dostane k souboru *autoexec.ncf,* kde je heslo v přímé řeči. Co můžeme tedy udělat pro bezpečnost? Jen to, že na jeho konec zařadíme mezeru nebo nějaký netisknutelný znak. Rconsole je umístěná v SYS:SYSTEM a SYS:PUBLIC, kde bychom ji neměli nechávat.

Všechny konfigurační soubory je vhodné přesunout na bezpečné místo. Jedná se o soubory s příponou ncf (jsou umístěny v adresáři SYS:SYSTEM). Je dobré je přesunout na jednotku C: na serveru. Ve verzi 4.x odstraňte public z root.

Jestliže instalujete NetWare, pak se při instalaci vytvoří tyto účty: „Supervisor, guest, admin a user_template“. Je nutné hned opatřit heslem supervisora a admin. Ochrana jmen účtů je velmi důležitá. Ten, kdo se dostane fyzicky k nějaké stanici a spustí lokálně přinesený program map.exe, může spustit programy ovladačů NetWare až po program netx. Jak? Lze napsat MAP G:=TARGET_SERVER/SYS:APPS a pak záleží na tom zda se mu podaří zadat správné ID. Jestliže je ID neplatné, objeví se nějaké chybové hlášení a server dotyčného nepřihlásí. V Netware 4.x jsou soubory fyzicky umístěny na jiném místě, než na svazku SYS:. Použitím programu rconsole a volby Scan Directory však můžeme uvidět soubory v SYS:_NETWARE.

Tabulka 5: *Databázové soubory NDS a jejich účel v NetWare*

Soubor	Účel
v a l u e . n d s	*část NDS*
b l o c k . n d s	*část NDS*
e n t r y . n d s	*část NDS*
p a r t i t i o . n d s	*typ oddílu NDS (replika, master)*
m l s . 0 0 0	*licence*
v a l l i c e n . d a t	*ověření licence*

Bezpečnost sítě proti neoprávněnému použití souborového serveru z pracovních stanic je zajištěna v rámci bezpečnostní politiky, přičemž správce má k dispozici programy:

„NW ADMINISTRATOR, FILER, NETADMIN A RIGHTS“.

Zhodnocení možnosti správce

Každý uživatel či skupina uživatelů musí mít svůj systém ochrany, který je tvořen:

- Login security (uživatelské jméno a heslo, účet uživatele)
- NDS security (NDS je databáze, ve které se nacházejí objekty, které jsou organizovány do stromové struktury. Je to distribuovaná databáze, která se nemusí nacházet na jednom serveru, využití repliky – kopie databáze a platí, cokoliv se změní v NDS, pak i v kopiích. Každý objekt má svůj kontext a svá práva v rámci NDS.
- Server console security (*zabezpečení proti nepovolaným přístupům*)

- File system security (*souborový systém ochrany*) nám umožňuje přesně definovat, jaké přístupy budou mít jednotliví uživatelé z NDS k tomuto systému, rozumí se vytvořit práva k souborům a adresářům (*Directory and file rights*), efektivní práva (*Effective rights*), přímé přidělení práv (*Trustees*), dědičnost (*Inheritance and Inheritance Rights Filters*).
- Printing security (*vytvoření tiskového serveru, vytváření tiskových front*).

Zda bude naše síť bezpečná či nikoliv, umožňuje protestovat program Kane Security Analyst (*KSA*), ale tento program není zadarmo, musí se zakoupit. Podrobnější informace lze získat na webowské stránce na adrese http://www.instrusion.com.

Než nastavíme program k protestování, musíme si uvědomit, které specifické slabiny chceme analyzovat. Naše možnosti jsou:

- Nastavení voleb pro přístup k účtům.
- Nastavení voleb pro přístup pro sílu hesel.
- Nastavení voleb pro řízení přístupu, testování přístupových práv uživatelů za účelem zjištění, zda někteří uživatelé nemají tato práva zbytečně široká.
- Nastavení voleb pro monitorování systému, řízení politiky prověřování auditu sítě, neúspěšné přihlašování, audit sítě může zároveň sledovat přístupy k souborům a objektům.
- Nastavení voleb pro důvěrnost dat, jak dobře jsou naše data chráněna.

Po nastavení voleb následuje spuštění analýzy a prohlídka seznamu rizik v síti. Hlavní rizika jsou označena jako „Top Risks“, kde patří například to, že správce správně neblokuje účty. Tento program nám umožní dostat se do systému, tím nám odhalí rizika a určí, jak se lépe zajistit proti nedovoleným přístupům. Je výhodné tento program spouštět pravidelně a tím se ujistit, že naše počítačová síť je bezpečná.

V této práci jsme se snažili podchytit nejdůležitější funkce ochrany systému proti všemu, co v síti může škodit. Nesmíme ale zapomenout, že Novell Netware je určen zejména pro poskytování služeb souborového a tiskového serveru. Správce instalace a provozu uděluje každému uživateli jeho přístupová práva k souborům a adresářům a jen správce je zodpovědný za sledování a správu sítě pomocí příslušných služebních programů.

Literatura

1. Aleš Křesťan: Novell Netware, průvodce síťovým prostředím, Grada, 1992
2. Internet, http://security-policy.org, http://ewos.be, http://www.si.co..au
3. Novell Education, Netware 4.11 Administrator, Course 520 Manual