Лабораторна робота №2

Налаштування політики безпеки операційної системи Windows XP SP2.

Мета: Навчитися правильно налаштовувати параметри безпеки операційної системи Windows XP SP2.

Теоретичні відомості

Навчитися захищати реєстр операційної системи (ОС) Windows XP є обов'язковою, але не достатньою умовою для правильного та безпечного функціонування операційної системи. Для успішної роботи у мережі необхідно не тільки встановити на свій комп'ютер сучасний антивірус з поновленою антивірусною базою та налаштувати міжмережевий екран (хай, навіть, і вбудований в ОС) але й грамотно налаштувати параметри самої операційної системи, що значно покращує її безпеку.

Як відомо, Службою безпеки України у 2007 році сертифіковано ОС Windows XP SP2 як операційну систему, придатну (за умови грамотного налаштування) для використання у системах обробки конфіденційної інформації. Які ж налаштування вважаються «грамотними»?

Нижче наведено рекомендації Національного банку України з подолання уразливостей операційної системи Windows XP SP2, які містяться у додатку до телеграми Нацбанку НБУ 24-112/2033. Детальніше ознайомитися з цими вимогами можна за адресою: http://www.broadband.org.ua/content/view/311/490/

Рекомендації наведено для ОС Windows XP Professional SP2, встановленої у конфігурації «за замовчуванням» і не уведеної в домен Active Directory.

Рекомендації розділено на кілька розділів згідно з типами параметрів операційної системи.

1. Загальні вимоги та рекомендації

1.1. У рекомендаціях забороняється надавати окремий комп'ютер (робочу станцію –РС) ОС Windows XP SP2 для віддаленого доступу іншим користувачам мережі. Обмін файлами між РС необхідно здійснювати лише **через файл-сервери**, а друк – **через спільний мережевий принтер** або **принт-сервер**.

Виконання цієї вимоги значно зменшує обсяг неконтрольованої інформації, що курсує мережею.

1.2. Адміністратор повинен заблокувати у BIOS комп'ютера наступні опції:

- включення комп'ютера через мережу (опція у BIOS має назву типу "Wake-Up by PCI card", "Wake ON LAN" тощо) **для запобігання навмисному або ненавмисному віддаленому його запуску**;

- після інсталювання ОС та необхідного програмного забезпечення (ПЗ) необхідно заблокувати завантаження РС з зовнішніх та знімних

пристроїв (накопичувача на гнучких дисках, FDD, накопичувача на оптичних дисках, CD-ROM, ZIP-Drive, USB-Flash тощо). **Це запобігає запуску альтернативної операційної системи, яка може ігнорувати чинний розподіл прав на файлову систему та надати повний доступ до інформації на локальних дисках;**

- обов'язковою вимогою є блокування доступу до BIOS та входу у систему за допомогою паролю.

1.3. Рекомендується при інсталюванні ОС не розділяти жорсткий диск на логічні, а створити один логічний диск «С:» з файловою системою NTFS. **У цьому разі ОС буде додатково блокувати доступ до усієї інформації як до системного диску.**

1.4. **Забороняється використання вбудованого механізму автоматичної/ручної відправки** до Microsoft звітів про помилки ОС Windows XP, для чого в меню *"Пуск" => "Панель управления" => "Переключение к классическому виду" => "Система" => "Дополнительно" => "Отчет об ошибках"* відмітити "Отключить отчет об ошибках".

1.5. **Необхідно заблокувати можливість доступу до РС під час увімкненої екранної заставки**, коли користувача немає на робочому місці. Для цього в реєстрі Windows в ключі: *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon* треба створити змінну *ScreenSaverGracePeriod* типу "REG_DWORD" та надати їй значення, рівне 0.

1.6. **Для запобігання автоматичного запуску програм** зі знімних та компакт-дисків (за наявності файлів типу autorun.inf) та ефективної боротьби з вірусами (які також використовують автоматичний запуск зі знімних носіїв) необхідно в ключі реєстру *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer* створити змінну "NoDriveTypeAutoRun" типу "REG_DWORD" та надати їй значення, рівне 0xFF. Якщо розділ "*Explorer*" не існує – створити його.

1.7. Для того, щоби адміністратор **міг ефективно слідкувати за подіями в системі**, необхідно встановити максимальне значення журналів аудиту не менше, ніж:

- "Безопасность" – 40960 Кбайт;
- "Система" – 20480 Кбайт;
- "Приложение" – 20480 Кбайт.

Журнали аудиту можна знайти за адресою: *«Пуск» → «Настройка» → «Панель управления» → «Администрирование» → «Просмотр событий»*. Змінити розмір можна, клацнувши по назві журналу правою кнопкою мишки, та вибравши «Свойства».

1.8. **Заборонити виконання команд альтернативних систем** (POSIX), для чого в ключі реєстру: *HKLM\System\CurrentControlSet\Control\SessionManager\SubSystems* видалити значення змінної реєстру "Optional".

1.9. Операційна система Windows XP при інсталяції автоматично створює приховані мережеві ресурси ("C$","D$" і т. ін.), які можуть використати зловмисники для подолання захисту комп'ютера. Отже

необхідно заборонити віддалений доступ до цих ресурсів, для чого в ключі реєстру
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters треба створити змінну реєстру "*AutoShareWks*" типу "REG_DWORD" та надати їй значення 0.

2. Вимоги, пов'язані з конфігурацією загальних параметрів облікових записів користувачів ОС

При інсталяції ОС Windows XP створює цілий ряд облікових записів зі стандартними назвами, наприклад, «Администратор», «Гость» і т.ін., які можуть бути використані зловмисниками для доступу в систему. Обліковий запис «Адміністратор», як правило, використовується лише для інсталяції ОС, а решту часу користувачі працюють під власними обліковими записами. Дуже небезпечно, коли зловмисник отримає доступ до системи з правами адміністратора, тому **облікові записи зі стандартними назвами необхідно перейменувати**.

Отже необхідно:

2.1. Перейменувати обліковий запис користувача "Администратор" або "Administrator".

2.2. Вилучити облікові записи користувачів "HelpAssistant" та "SUPPORT_388945a0".

2.3. Встановити обліковому запису користувача "Гость" пароль та заблокувати його.

2.4. Встановити наступні параметри групової політики. Дії виконуються за допомогою утиліти "Групповая политика" (gpedit.msc):

– в розділі "*Конфигурация пользователя/Административные шаблоны /Рабочий стол*" встановити для параметру "Не добавлять общие папки, из которых открыты документы, в "Сетевое окружение"" значення – "включен";

– в розділі "*Конфигурация пользователя/Административные шаблоны /Панель управления/Экран*" встановити для параметра "*Использовать парольную защиту для экранных заставок*" значення – "включен";

– в розділі "*Конфигурация пользователя/Административные шаблоны /Панель управления/Экран*" встановити для параметра "*Использовать экранные заставки*" значення – "включен";

– в розділі "*Конфигурация пользователя/Административные шаблоны /Панель управления/Экран*" встановити для параметра "*Таймаут экранной заставки*" значення – "включен", та ввести у полі "Секунд" значення "600".

2.5. Для облікового запису користувача "AdminARM" зняти відмітку "*Автоматический поиск сетевых папок и принтеров*" в "*Мой компьютер" => "Свойства папки" => "Вид*".

2.6. Для облікового запису користувача "AdminARM" встановити політику зміни паролю відповідно до прийнятої в організації політики безпеки.

3. Рекомендації до конфігурування "Локальних політик безпеки"

3.1. Майкрософт рекомендує таку парольну політику безпеки:

(*Панель управления => Администрирование => Локальная политика безопасности => Политика учетных записей => Политика паролей*)

Політика	Параметр безпеки
Макс. срок действия пароля	42 дні
Мин. длина пароля	6 символів
Мин. срок действия пароля	2 дні
Пароль должен отвечать требованиям сложности	«включен»
Требовать неповторяемость паролей	24 хранимых паролей
Хранить пароли всех пользователей в домене, используя обратимое шифрование	«отключен»

«Максимальный срок действия пароля» - це той максимальний період, коли система змусить користувача змінити поточний пароль. «Минимальный срок действия пароля» - той період часу, на протязі якого користувач не зможе змінити поточний пароль (ця вимога перешкоджає занадто частій зміні паролів). «Минимальная длина пароля» - обмеження на мінімальну довжину пароля (перешкоджає легкому підбиранню паролів). «Пароль должен отвечать требованиям сложности» - вимоги до складності паролів. Якщо ця політика задіяна, система буде перевіряти пароль користувача на дотримання таких правил:

- Пароль не повинен містити назву облікового запису користувача або фрагменти назви довжиною більше двох символів.
- Довжина пароля не повинна бути меншою за шість символів.
- Пароль повинен містити символи трьох з чотирьох наступних категорій: латинські великі літери (A - Z); латинські малі літери (a - z); цифри (0 - 9); додаткові спеціальні символи (наприклад, !, $, #, %).

Перевірка дотримання цих вимог виконується під час зміни або створення паролів.

«Требовать неповторяемость паролей» - система зберігає 24 останніх паролі користувача для того, щоби вони не повторювалися. «Хранить пароли всех пользователей в домене, используя обратимое шифрование» необхідно задіяти лише для підтримки програмного забезпечення, що використовує протоколи, яким для перевірки автентичності необхідно знати пароль користувача. Однак використання **зворотного шифрування** значно послаблює захист системи, а отже **настійливо не рекомендується**.

3.2. Політика блокування облікового запису (*Панель управления => Администрирование => Локальная политика безопасности => Политика учетных записей => Политика блокировки учетной записи*):

Політика	Параметр безпеки
Блокировка учетной записи на	30 хвилин

Пороговое значение блокировки	3 помилки входу до системи
Сброс счетчика блокировки через	30 хвилин

3.3. Встановити наступні параметри безпеки (*Панель управления => Администрирование => Локальная политика безопасности => Локальные политики => Параметры безопасности*):

Політика	**Параметр безпеки**
Интерактивный вход в систему: напоминать пользователям об стечении срока действия пароля заранее	10 діб
Интерактивный вход в систему: не отображать последнего имени пользователя	«включен»
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	«включен»
Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	«включен»
Сетевая безопасность: уровень проверки подлинности LAN Manager	"Отправлять только NTLM ответ"
Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля	«включен»
Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей	«гостевая»
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	«включен»
Сетевой доступ: разрешать анонимный доступ к общим ресурсам	вилучити значення

3.4. У розділі "*Локальные политики/Назначение прав пользователя*" встановити наступне:

Політика	**Параметр безпеки**
Запретить вход в систему через службу терминалов	«Все»
Отказ в доступе к компьютеру из сети	додати в перелік групу "Администраторы"

3.5. У розділі "*Локальные политики/Политика аудита*" встановити наступне:

Політика	Параметр безпеки
Аудит входа в систему	"Успех" та "Отказ"
Аудит событий входа в систему	"Успех" та "Отказ"
Аудит изменений политики	"Успех" та "Отказ"
Аудит управления учетными записями	"Успех" та "Отказ"
Аудит использования привилегий	"Отказ"
Аудит системных событий	"Успех" та "Отказ"

4. Рекомендації до конфігурування служб ОС

Національний банк України рекомендує **відключити наступні служби** операційної системи (дії виконуються за допомогою утиліти «Служби» (*Панель управления => Администрирование => Службы*):

Служба	Тип запуску
Оповещатель (відправляє обраним користувачам та комп'ютерам адміністративні повідомлення)	"отключено"
NetMeeting Remote Desktop Sharing (дозволяє досвідченим користувачам отримувати доступ до робочого столу Windows через корпоративну мережу з використанням NetMeeting)	"отключено"
Диспетчер сеанса справки для удаленного рабочего стола (керує можливостями Віддаленого помічника: після зупинки цієї служби Віддалений помічник буде недоступним)	"отключено"
Удаленный реестр (дозволяє віддаленим користувачам змінювати параметри реєстру на цьому комп'ютері; якщо цю службу зупинено, реєстр можуть змінювати лише локальні користувачі, які працюють на цьому комп'ютері)	"отключено"
Служба обнаружения SSDP (виявляє UPnP-пристрої у домашній мережі)	"отключено"
Узел универсальных PnP-устройств (підтримка універсальних PnP-пристроїв)	"отключено"
Службы терминалов (надає	"отключено"

можливість кільком користувачам інтерактивно під'єднуватися до комп'ютера, відображає робочий стіл та програми на віддалених комп'ютерах; служить основою для віддаленого робочого столу (включаючи віддалене адміністрування), швидкого перемикання користувачів, віддаленого помічника та служб терміналів)	
Служба индексирования (індексування вмісту та властивостей файлів на локальному та віддалених комп'ютерах, забезпечує швидкий доступ до файлів за допомогою гнучкої мови запитів)	"отключено"
Автоматическое обновление (забезпечує завантаження та встановлення поновлень Windows)	"отключено"

5. Рекомендації до конфігурування параметрів мережевого доступу

5.1. Нацбанк України рекомендує заборонити віддалений доступ до реєстру, для чого для ключа реєстру: *HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\SecurePipeServers\Winreg* встановити такі права доступу:

- для групи "Администраторы" та "Система" – право "Полный доступ";
- для групи "LOCAL SERVICE" – право "Чтение"
- для усіх інших користувачів та груп – вилучити їх з переліку груп та користувачів, яким надано доступ.

5.2. Відключити віддалений доступ до комп'ютера, для чого в меню "Пуск" => "Панель управления" => "Система" => "Удалённое использование" зняти відмітку з "Разрешить удалённый доступ к этому компьютеру" та з "Разрешить отправку приглашения удалённому помощнику".

5.3. Заборонити використання SSDP (Simple Service Discovery Protocol and UpnP Universal Plug and Play), для чого в ключі реєстру: *HKEY_LOCAL_ MACHINE\Software\Microsoft\DirectPlayNATHelp\DPNHUPnP* створити змінну реєстру "UPnPMode" типу "REG_DWORD" та надати їй значення 2.

5.4. Необхідно сконфігурувати вбудований брандмауер Windows" відповідно до прийнятої в організації політики безпеки, а також вимог встановленого ПЗ щодо роботи з мережею.

6. Рекомендації, пов'язані з вилученням компонентів ОС

Нацбанк настійливо рекомендує вилучити наступні компоненти ОС:

- "Сетевые службы";
- "Игры в Интернете".

Для цього відкрийте *«Панель управления» => «Установка и удаление программ» => «Установка компонентов Windows»* та зніміть «галочку» з «Сетевые службы». "Игры в Интернете" знаходяться у *«Панель управления» => «Установка и удаление программ» => «Установка компонентов Windows» => «Стандартне и служебные програмы» => «Игры»*.

Хід роботи

Для виконання лабораторної роботи необхідно зробити наступне:

1. Встановіть на комп'ютері або у віртуальну машину операційну систему Windows XP Professional SP2 стандартного випуску Microsoft.
2. Встановіть на комп'ютері або у віртуальну машину діагностичне програмне забезпечення LanSpy 2.0 від LanTricks та Microsoft Baseline Security Analyzer 2.0.1.
3. Проскануйте локальний комп'ютер (localhost) за допомогою LanSpy (натиснувши F3) та збережіть результати у HTML- або XML-форматі.
4. Проскануйте комп'ютер за допомогою Microsoft Baseline Security Analyzer 2.0.1 та збережіть результати для порівняння.
5. Налаштуйте параметри безпеки операційної системи Вашого комп'ютера згідно з вимогами Нацбанку (за винятком пунктів, пов'язаних з модифікацією BIOS), які викладено у теоретичній частині.
6. Повторно проскануйте Ваш комп'ютер за допомогою LanSpy та Microsoft Baseline Security Analyzer 2.0.1 і порівняйте результати з попередніми, звернувши особливу увагу на ті пункти звіту, параметри яких налаштовувалися (Локальне группы, Удаленное управление, Настройки безопасности, Разделяемые ресурсы, Системне службы).

Звіт з лабораторної роботи

1. Напишіть звіт з лабораторної роботи, в якому проаналізуйте параметри безпеки Вашого комп'ютера до та після налаштування. Зробіть висновок про покращення (або погіршення) безпеки комп'ютера та визначте, в чому саме відбулися позитивні (або негативні) зміни.
2. Крім цього звіт повинен містити протокол Ваших дій та результати сканування обома діагностичними програмами до та після зміни налаштувань.
3. Дайте відповіді на контрольні запитання та захистіть звіт з лабораторної роботи.

Контрольні запитання

1. Які вимоги висуваються до налаштування BIOS з метою захисту його від запуску сторонніми особами?
2. Як можна захистити комп'ютер від несанкціонованого доступу під час відсутності користувача на робочому місці?
3. Які приховані мережеві ресурси було створено операційною системою Windows XP SP2 під час інсталяції? Як Ви запобігли доступу до них?
4. Як можна підвищити ефективність спостереження за подіями у системі?
5. Навіщо висуваються вимоги до блокування або перейменування стандартних облікових записів? Перелічіть назви облікових записів, які Ви вилучили, перейменували або заблокували.
6. Які вимоги висуваються до політики парольного захисту?
7. Які вимоги висуваються до політики блокування облікових записів?
8. Які служби операційної системи рекомендується відключити? Чому?
9. Які вимоги висуваються до захисту реєстру Windows від віддаленого доступу? Як Ви це зробили?
10. Які компоненти Windows необхідно вилучити? Для чого це робиться?
11. Опишіть призначення та можливості діагностичного програмного забезпечення LanSpy та Microsoft Baseline Security Analyzer?

Література

1. Безопасная Windows XP: Как не попасть на трафик? Секретные материалы" Национального банка Украины. http://www.broadband.org.ua/content/view/311/490/
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.:Наука и техника, 2004.
3. Шеховцов В.А. Операційні системи. – СПб:BHV, 2006. – 576 с.