УДК 004.056

О.М. Юдін[1], П.М. Гроза[2], С.В. Сомов[2], О.В. Тесленко[3]

[1]*Полтавський університет споживчої кооперації, Полтава*
[2]*Полтавський національний технічний університет ім. Ю. Кондратюка, Полтава*
[3]*Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*

ОГЛЯД ЗАСОБІВ І ТЕХНОЛОГІЙ КОНТРОЛЮ ВУЗЛІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В статі розглянуті засоби оцінки та настройка безпеки вузлів комп'ютерної мережі, пошук і усунення уразливостей, а також технології CISCO и Microsoft, що дозволяють контролювати підключення віддаленого комп'ютера до корпоративної мережі.

Ключові слова: *шаблони безпеки, засоби аналізу захищеності, сканер безпеки, системи управління оновленнями, контроль доступу до корпоративної мережі, протокол автоматизації управління даними безпеки.*

Вступ

Інформаційні технології (ІТ) стали невід'ємною частиною нашого життя й істотно впливають на успіх бізнесу, його конкурентну здатність як усередині країни, так і на світовій арені. По даним Департаменту праці США довгостроковий ріст економіки, починаючи з 1948 року й протягом 50 років, забезпечувався розвитком технологій виробництва, однак за останні 10 років ця роль перейшла до інформаційних і телекомунікаційних технологій, які здатні забезпечити більше ефективне рішення питань організації бізнес-процесів. По оцінках західних експертів у даний момент доля внеску ІТ у збільшення продуктивності праці становить 52% [1].

В умовах зростання конкурентної боротьби, а, отже, і значимості інформаційних і телекомунікаційних технологій, особливого значення набуває завдання забезпечення необхідного рівня захищеності комп'ютерних мереж. Істотний вплив на захищеність мережі робить наявність уразливостей – слабких місць у системах і додатках, використання яких зловмисником може привести до реалізації загрози, а також неправильне конфігурування програмних і апаратних засобів, що становлять її інфраструктуру. Сьогодні прийнято характеризувати таку конфігурацію, її відповідність установленим корпоративним стандартам і політикам безпеки, терміном «здоров'я» (health). Відповідно контроль за «здоров'ям» вузла мережі допомагає захистити не тільки його, але й комп'ютерну мережу в цілому. У даній статті приводиться короткий огляд засобів і технологій, які використовуються для здійснення контролю за «здоров'ям» вузлів комп'ютерної мережі.

Основний розділ

Шаблони безпеки

Локальні користувачі й адміністратори комп'ютерних мереж можуть оцінити й настроїти безпеку своїх систем за допомогою шаблонів безпеки операційних систем (ОС) Windows, які вперше з'явилися в пакеті оновлень Service Pack 4 (SP4) для ОС Windows NT 4.0 [2]. Шаблон безпеки є текстовим файлом, що містить параметри безпеки, його можна застосувати єдиною командою, що дозволяє практично моментально настроїти безпеку окремого комп'ютера або мережі (за допомогою групових політик у домені). Недолік використання шаблонів полягає в тім, що вони не є засобом, що забезпечує постійний контроль безпеки системи. Єдиний спосіб гарантувати, що параметри залишаються в силі, - регулярно застосовувати шаблон вручну або створити групову політику, що використовує шаблон. Але використовувати групові політики можна тільки при наявності домену. Інший недолік шаблонів полягає в тім, що вони дозволяють оцінити й настроїти тільки параметри безпеки системи й зовсім не дозволяють оцінити її захищеність: не перевіряється наявність відновлень і заплаток для ОС і встановленого програмного забезпечення, а також не перевіряється наявність антивірусу й актуальність використовуваних сигнатурних баз.

Засоби аналізу захищеності

Для пошуку уразливостей адміністратор комп'ютерної мережі використовує системи аналізу захищеності. В 2008 році було знайдено й опубліковане 8973 повідомлень про вразливості. По підрахунках компанії McAfee, збиток від діяльності кіберзлочинців склав біля одного трильйона доларів. Однак розроблювачі програмного забезпечення як і раніше серйозно не замислюються над подібними показниками. Підтвердженням цьому є випуск корпорацією Microsoft пакета оновлень, що став самим масштабним за останні п'ять років: пакет усуває 29 уразливостей, 23 з яких мають статус критичні [3].

Проведений аналіз публікацій [4, 5] дозволяє класифікувати системи й засоби аналізу захищеності в такий спосіб (рис. 1).

Переваги й недоліки ЗАЗ різного типу розглядалися в [6] і наведені в табл. 1.

Коротка характеристика основних сканерів безпеки наведена в табл. 2 [7].

Таблиця 1

Переваги й недоліки засобів аналізу захищеності

	Засоби аналізу захищеності				
	Активні				Пасивні
	рівня мережі	рівня ОС	рівня додатків	централізованого контролю й аудита	
ПЕРЕВАГИ	– виявляють уразливості на великій кількості різнорідних платформ і систем, що підтримують уніфіковані мережні протоколи; – незалежні від платформ і систем, які використовуються у мережі; – відсутні агенти на вузлах, що скануються – дозволяє легко використовувати ці засоби з організаційної точки зору.	– забезпечують створення дуже точної, конкретної для даного вузла картини уразливостей; – виявляють уразливості, які були пропущені системами аналізу захищеності на рівні мережі.	– забезпечують створення дуже точної, конкретної для даного вузла картини уразливостей; – виявляють уразливості, які були пропущені системами аналізу захищеності на рівні мережі.	– контролюють засоби захисту вузлів комп'ютерної мережі; – є можливість збільшення типів об'єктів, які може контролювати система.	– пасивно прослуховують мережний трафік, не створюючи додаткового, не бажаного навантаження на елементи інфраструктури мережі; – реагують на динаміку змін, що відбуваються в мережі.
НЕДОЛІКИ	– не враховують уразливості, властиві рівням вище мережного, тому мають меншу точність, чим засоби аналізу захищеності на рівні ОС, СУБД і додатків; – можуть здійснювати вплив на продуктивність мережі і її характеристики – при невірній експлуатації ці засоби можуть порушити функціональність деяких вузлів мережі; – орієнтовані не на всі протоколи (дуже мало програм, які працюють із IPX).	– методи аналізу залежать від типу конкретної платформи й, таким чином, мають потребу в точній конфігурації кожного типу вузла, що використовується; – експлуатація й відновлення засобу часто вимагає більше зусиль, чим при аналізі захищеності на рівні мережі; – не можуть використовуватися для обладнання, що не має операційної системи.	– дозволяють виявляти уразливості тільки для найпоширенішого прикладного програмного забезпечення.	– відсутній контроль захищеності робочих станцій мережі й програмних засобів вузлів, на яких установлені дані засоби; – відсутня можливість відновлення бази даних уразливостей; – відсутнє спостереження за завантаженням вузлів і ліній зв'язку мережі, трафіком контролю; – відсутня можливість установлення пріоритету перевірки вузлів.	– не можуть виявити всього того, що здатні побачити активні сканери.

ISSN 1997-9568

Таблиця 2

Основні характеристики сканерів уразливостей

Назва	Nessus	Xspider	ISS	SARA	MBSA	Nikto
Поточна версія	4.0.0	7.5	7.2	7.8.4	2.0.1	1.3.6
Сайт розробника	http://www.nessus.org	http://ptsecurity.ru/	http://www.iss.net	http://www-arc.com	http://www.microsoft.com	ttp://www.cirt.net
Операційна система	Linux, Unix, Mac OS X, Windows (32 bits)	Windows	Windows 2000 SP4 і більше пізні	Unix, Linux	Windows 2000 SP3 і більш пізні версії	Windows, Unix, Linux
Відмінні риси	Мова для написання плагінів - NASL. Розподілена архітектура. У звіті досить багато службової інформації про плагіни.	Найпоширеніший сканер у Росії. Ефективні евристичні алгоритми виявлення уразливостей і визначення сервісів. Перевірки веб-додатків. Низький рівень	Розподілена архітектура. Велика кількість передустановлених політик і видів звітів. Здатний	Security Auditor's Research Assistant (SARA) є розвитком одного з найперших сканерів SATAN. Має високу швидкість роботи й низький рівень помилкових спрацьовувань.	Служить для виявлення оновлень, які необхідно встановити на продукти Microsoft (в основному ОС і їхні компоненти).	Сканер веб-серверів. Представляє собою скрип на PERL. Є невидимий режим роботи (можна
Додаткове ПО	MSXML4		MSDE разом з MDAC і Sun Java 2 Runtime	–	MSXML; Windows Update Agent 2.0	Підтримка PERL і модулі NET::SSL і LibWhisker
GUI	+	+	+	+	+	–
Підтримка командного рядка	+	+	+	+	+	+
Розклад	–	+	+	–	–	–
Формат звітів	mht, html, pdf, xml	html, rtf	Більше 70 типів звітів у форматах	xml, ms word, csv, vts	xml, text	html, txt, cvs
База сигнатур	При установленні 14999 плагінів для сканування. На сайті	>6000	>1500	Немає даних	Незастосовне	>3300
Частота регулярних оновлень	–	Щоденне	–	Раз на місяць	Раз на місяць	–
Ціна повної	1200$ у рік	від 7400 руб.	від 1500$	free	free	free
Обмеження безкоштовної версії	Автоматичне відновлення тільки через 7 днів і відсутність підтримки	Немає оновлень. Немає частини перевірок на Dos-уразливості й перевірок з використанням евристичних механізмів.	Можливість сканування тільки локальної машини	Незастосовне	Незастосовне	Незастосовне
База сигнатур	При установці 14999 плагінів для сканування. На сайті	>6000	>1500	Немає даних	Незастосовне	>3300
OpenSource	–	–	–	–	–	+

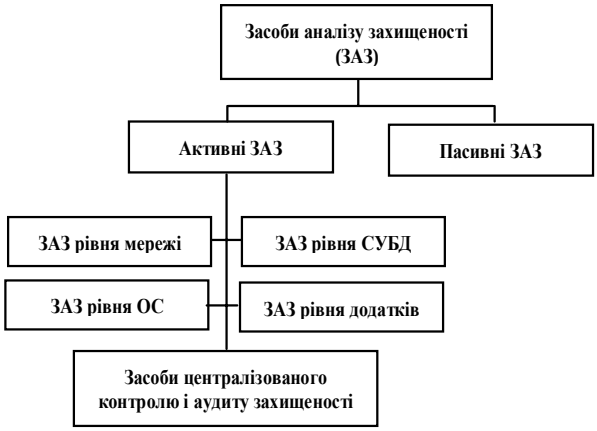

Рис. 1. Класифікація засобів аналізу захищеності

За результатами дослідження, кращим сканером безпеки визнаний MaxPatrol (XSpider) російської компанії Positive Technologies. Сканер забезпечує якісну ідентифікацію сервісів і додатків, має досить повну базу перевірок, зручний і логічний інтерфейс. У п'ятірку кращих сканерів безпеки входять Nessus, Retina, Internet Scanner, GFI LanGuard [8]. Усунення знайдених уразливостей реалізується за допомогою пакетів оновлень і "заплаток". Установлення пакетів оновлень дозволяють виконати деякі сканери безпеки, наприклад, GFI LanGuard, разом з тим існують і спеціалізовані рішення, що дозволяють підвищити рівень захищеності вузлів комп'ютерної мережі – системи керування оновленнями.

Для локального комп'ютера в середовищі операційної системи Windows використовується спеціальна служба – Windows Update. Для керування оновленнями в комп'ютерній мережі використовується серверний компонент – WUS (Windows Update Services) [9]. WUS крім операційних систем від Microsoft забезпечує підтримку широкого спектра різних програмних продуктів, список яких постійно розширюється. Доступна класифікація оновлень - крім традиційних заплаток безпеки, виділені кумулятивні пакети оновлень і Service Pack, драйвери, допоміжні утиліти, документація. На жаль, типи оновлень вибираються тільки глобально, без прив'язки до конкретних продуктів. Механізм установки заплати включає два етапи: кожна заплата може бути "схвалена" або винятково для визначення потреби в ній, або вже остаточно, для поширення на комп'ютери, що обслуговуються.

На другому етапі провадиться завантаження в локальний архів реальних інсталяційних модулів. Є можливість дозволу окремих категорій заплаток для різних груп комп'ютерів, що обслуговуються. Адміністратор великої мережі може створити спеціальну тестову групу для «обкатування» заплаток, які будуть установлюватися автоматично. Після з'ясування всіх можливих особливостей, установлення заплаток «схвалюється» і дозволяється для головної групи робочих станцій.

Програма надає досить докладну інформацію про всі вузли комп'ютерної мережі: можна перевірити їхній поточний статус, вивчити список установлених і необхідних заплаток. Також надається зведена інформація, що дозволяє оцінити загальну обстановку буквально з одного погляду. Крім того, в WUS реалізована на найпростішому рівні інвентаризація апаратного забезпечення (що актуально при розповсюдженні драйверів).

Наступна технологія з'явилася у відповідь на впровадження в багатьох організаціях концепції віртуального офісу й на динамічний характер ведення сучасного бізнесу, що вимагає залучення співробітників компанії у відповідні процеси незалежно від його місця знаходження [10]. Внаслідок цього віддалені підключення до корпоративних систем і мереж можуть проводитися звідки завгодно, у тому числі з публічних комп'ютерів, установлених в інтернет-кафе або готелях. Крім того, у компаній є партнери й замовники, у яких також періодично виникає необхідність у доступі до певних корпоративних ресурсів. Однак все це веде до розмитості периметра мережі, виникає небезпека вірусної атаки на мережу підприємства, якщо вузол, що підключається, уже заражений.

Сутність даної технології полягає в тім, що перш, ніж дозволити підключення віддаленого комп'ютера до корпоративної мережі, виконується оцінка відповідності конфігурації його програмного забезпечення встановленим вимогам і політикам безпеки. Зокрема можуть перевірятися: наявність певних системних служб, їх настроювання, наявність антивірусного й антишпигунського ПО й актуальність їхніх оновлень, наявність установлених критичних оновлень для ОС.

У даний момент існує безліч варіантів реалізації даного підходу від різних виробників: Microsoft, Symantec, Sophos, Juniper, CISCO, Trend Micro. Корпорація Cisco пропонує два підходи до впровадження даної технології, що називається Network Admission Control (NAC): на базі пристроїв (NAC Appliance) і на базі архітектури (NAC Framework).

Network Admission Control

До складу входять наступні компоненти:

- Cisco Trust Agent (CTA) – програма, установлена на кінцевій системі й збирає інформацію про стан безпеки від спеціалізованих продуктів, які надають інформацію про версію операційної системи й наявності останніх заплаток;
- Network Access Devices (NAD) – пристрої, що забезпечують доступ до мережі: маршрутизатори, комутатори, бездротові точки доступу й пристрої безпеки, що нав'язують політику контролю за доступом;
- Cisco Secure Access Control Server (ACS) – сервери політик, що обробляють отриману від при-

строїв доступу до мережі інформацію про кінцеві системи, і на її основі виробляють рішення про застосування тієї або іншої політики доступу;

- CiscoWorks VPN/Security Management Solution (VMS) – система керування забезпечує підтримку елементів NAC, а CiscoWorks Security Information Manager Solution (SIMS) – інструменти по моніторингу й оповіщенню.

NAC Framework. Архітектурно-орієнтований підхід, дозволяє інтегрувати мережні технології Cisco, антивірусні пакети й інші програмні продукти від сторонніх виробників для захисту мережі й управління мережею. У даний момент NAC Framework поєднує інтелектуальну мережну інфраструктуру Cisco з рішеннями більше 50 розроблювачів провідних програмних засобів боротьби з вірусами, безпеки й управління. Впровадження NAC Framework є оптимальним для великомасштабної корпоративної мережі, у якій використовується IP-Телефонія й протокол 802.1x або планується їхнє впровадження; мережа має комплексне робоче середовище (LAN/WAN/бездротові ресурси); інфраструктура мережі повністю або в основному базується на технологіях Cisco. Крім того, необхідна сумісність із рішеннями партнерів по NAC в області забезпечення безпеки й управління.

Порядок взаємодії компонентів NAC при використанні інтегрованого підходу до контролю доступу показаний на рис. 2. Компоненти NAC взаємодіють у такий спосіб:

1) комп'ютер посилає пакет через маршрутизатор (NAD) з підтримкою NAC;

2) NAD надсилає запит про стан безпеки на клієнті, CTA посилає звіт про поточний стан безпеки;

3) маршрутизатор пересилає інформацію про стан на ACS;

4) ACS запитує перевірку стану безпеки;

5) сервер визначення поточного стану повертає результати перевірки;

6) відповідно до результатів, ACS посилає маршрутизатору команду, щоб дозволити/заборонити або обмежити доступ;

7) клієнтові пересилається відповідь із результатами перевірки.

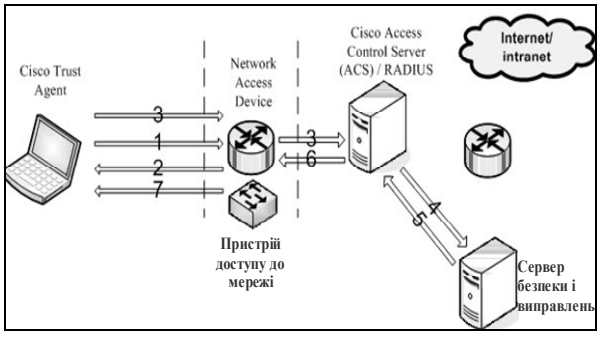

Рис. 2. Порядок взаємодії компонент NAC Framework

За підсумками процесу перевірки клієнт попадає в одну з категорій:

- Healthy (здоровий) – поточний стан безпеки на клієнті повністю відповідає певній політиці;
- Checkup (має потребу у оновленні) – на клієнті є деякі файли, що не повністю відповідають політиці; користувачі повинні виконати оновлення, однак ніяких обмежень у доступі не накладається;
- Quarantine (карантин) – користувач повинен негайно виконати оновлення, може бути завантажений ACL, що дозволяє доступ тільки до сервера оновлень;
- Infected (заражений вірусами) – доступ обмежується за допомогою ACL;
- Unknown (невідомо) – клієнт не відповідає на запити.

NAC Appliance. Для мереж, у яких обладнання не має вбудованої підтримки NAC, корпорація пропонує рішення у вигляді сімейства апаратно-програмних засобів під назвою Cisco Clean Access (NAC Appliance), що складається із трьох продуктів:

- Cisco Clean Access Server (CAS);
- Cisco Clean Access Manager (CAM);
- Cisco Clean Access Agent (CAA).

CAS доступний у вигляді програмного продукту або у вигляді пристрою й може працювати у двох режимах. У режимі «in-band» трафік проходить через CAS (рис. 3), і, якщо клієнт задовольняє політиці безпеки, то його трафік пропускається, якщо ж ні - блокується. Запити клієнта можуть перенаправлятися на web-сервер, що містить необхідні файли для виправлення. У режимі «out-of-band» трафік не проходить через CAS (рис. 4), а перевірка виконується при взаємодії мережного пристрою й CAS. Це дозволяє обробляти більший трафік у порівнянні з режимом «in-hand».

Перевірка клієнта може здійснюватися за допомогою мережного сканера Nessus і за допомогою CAA. Для роботи в режимі «out-of-band» необхідна підтримка з боку мережного обладнання, причому CAS управляє комутаторами за допомогою протоколу SNMP. У режимі «out-of-band» підтримуються комутатори Cisco Catalyst.

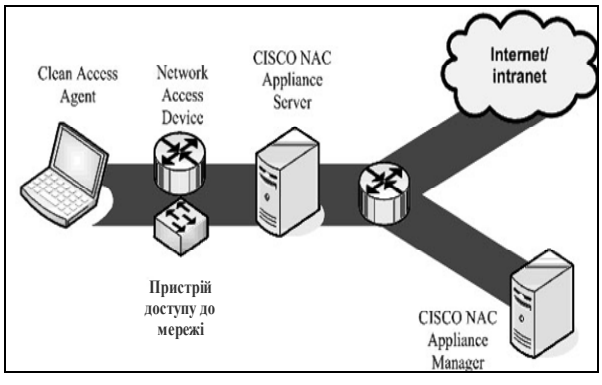

Рис. 3. Організація роботи компонентів NAC Appliance у режимі “in-band”

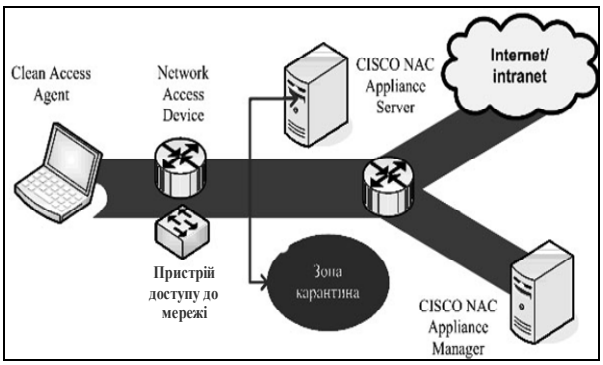

Рис. 4. Організація роботи компонентів NAC Appliance у режимі “out-of-band”

CAM також пропонується у вигляді пристрою або програмного продукту й призначений для централізації управління CAS.

CAA – необов'язковий елемент, що дозволяє виконувати вхід у мережу без використання браузера й здійснювати більш глибоку перевірку стану безпеки клієнта.

NAC Appliance рекомендують використовувати в локальних мережах, що не підтримують протокол 802.1x, бездротових мережах, мережах філій, віддалених офісів. Дане рішення підходить для тих мереж, де застосовується централізоване робоче середовище й управління, а доступ до мережі здійснюється з некерованих комп'ютерів (наприклад, відвідувачів, підрядників або учнів). Також рішення оптимально для застосування в неоднорідній (при наявності продуктів багатьох виробників) мережній інфраструктурі.

Network Access Protection

У продуктах Microsoft технологія контролю за доступом до корпоративної мережі одержала назву Network Access Protection (NAP). Вона реалізована (рис. 5) в ОС Windows Server 2008, Windows VISTA, Windows XP SP3 [3].

Основним елементом, що здійснює перевірку вузла, у цьому випадку, є Network Policy Server (NPS) – служба, що входить до складу Windows Server 2008. NPS здійснює аутентифікацію й авторизацію спроби мережного підключення, ґрунтуючись на політиках безпеки, визначає, чи можна вузлу підключитися до мережі. Одним з компонентів даної служби є політики оцінки стану («здоров'я») системи (Health Policies).

Таким чином, використання NAC/NAP дозволяє:

– забезпечити доступ до мережі тільки вузлам, конфігурація яких відповідає політиці безпеки;

– локалізувати заражені машини й блокувати тим самим вірусну епідемію;

– полегшити процес відновлення програмного забезпечення;

– знизити сукупну вартість володіння системою інформаційної безпеки.

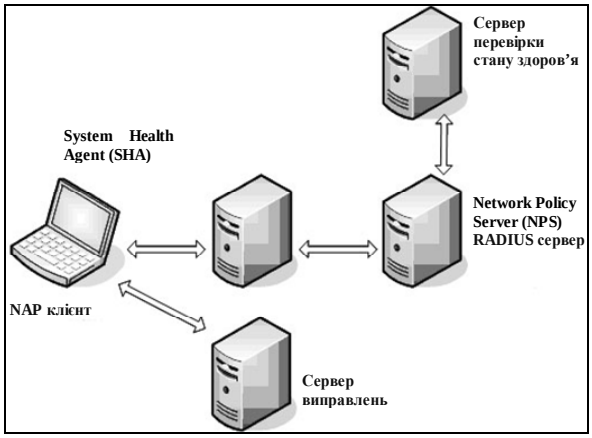

Рис. 5. Порядок взаємодії компонентів NAP

NAC/NAP дозволяє обслуговувати комп'ютери не тільки віддалених співробітників, але й звичайні робочі станції мережі, які тривалий час можуть перебувати у відключеному стані або конфігурація яких може бути змінена невідомим вірусом або самим співробітником. Періодичні перевірки «здоров'я» вузлів мережі дозволяють вчасно виявити всі невідповідності й внести необхідні корективи безпосередньо в процесі моніторингу.

Відповідно до недавнього звіту Network Access Control in 2009 and Beyond ("Управління мережним доступом в 2009-му і наступних роках"), опублікованому Gartner, в 80% випадків NAC використовуються для того, щоб обмежити доступ користувачам, що мають право підключатися до мережі, але не є постійними співробітниками, яким гарантований повний доступ [13]. Однак управління мережним доступом застосовується для перевірки відповідності кінцевих точок базовому профілю досить рідко, і тільки в 15% випадків на основі оцінки стану кінцевої точки обмежується доступ до мережі.

На сьогоднішній день уже є організації, що успішно впровадили технологію Network Access Protection і використовують її у своїй повсякденній роботі. Одною з таких організацій став уряд Фултона (США). Реалізація даного проекту по впровадженню NAP для більш ніж 5000 співробітників дозволила знизити навантаження на службу технічної підтримки організації на 75%, а економія на підтримці IT-інфраструктури склала $1570000 щорічно [14].

Security Content Automation Protocol

Розглянемо Security Content Automation Protocol (SCAP) – протокол автоматизації управління даними безпеки. Протокол SCAP - це набір відкритих стандартів, що визначають технічні специфікації для подання й обміну даними по безпеці [15]. Ці дані можуть бути використані для кількох цілей, включаючи автоматизацію процесу пошуку уразливостей, оцінки відповідності технічних механізмів контролю й виміру рівня захищеності. SCAP складається з наступних стандартів:

- типові уразливості й помилки конфігурації (Common Vulnerabilities and Exposures, CVE);
- список типових конфігурацій (Common Configuration Enumeration, CCE);
- список типових платформ (Common Platform Enumeration, CPE);
- єдина система визначення величини уразливості (Common Vulnerability Scoring System, CVSS);
- розширюваний формат опису списку перевірки конфігурації (Extensible Configuration Checklist Description Format, XCCDF);
- відкрита мова опису уразливостей і оцінки (Open Vulnerability and Assessment Language, OVAL).

SCAP є частиною більше широкої програми автоматизації інформаційної безпеки (ISAP). Дана програма створена для виконання завдань автоматизації процесів впровадження й перевірки механізмів безпеки інформаційних систем (ІС). Цілі ISAP містять у собі розробку вимог для автоматичного обміну даними інформаційної безпеки, настроювання й управління базовими конфігураціями для різних IT-продуктів, оцінку ІС і перевірку відповідності вимогам, використання стандартних метрик для оцінки й підрахунку інтегрального впливу уразливостей, усунення виявлених уразливостей.

Сайт SCAP містить XML файли у форматі SCAP для різних операційних систем і додатків. Національний інститут стандартів і технологій (NIST), разом з державними й комерційними партнерами, переводить деякі з популярних списків перевірки у формат SCAP, для використання в автоматизованих інструментах. Сайт SCAP містить опис засобів для автоматичної перевірки відповідності конфігурації ОС Windows XP і Windows Vista рекомендованим інструкціям, які розроблені провідними постачальниками рішень в області безпеки, наприклад, McAfee, Symantec, Qualys, Shavlik. Після перевірки правильності настроювання системи, можна провести тестування для перевірки того, що інші додатки працюють коректно й не змінюють базових настроювань безпеки. Це дозволяє виявити вплив негативного ефекту на функціональність системи до її промислового впровадження.

Висновок

Таким чином, огляд розглянутих засобів і технологій перевірки «здоров'я» вузлів комп'ютерної мережі дозволяє простежити їх еволюційний розвиток. Оцінити параметри конфігурації операційної системи на відповідність необхідному рівню безпеки дозволяють убудовані інструменти аналізу ОС - шаблони безпеки. Однак шаблони безпеки не дозволяють одержати інформацію щодо загроз іншого типу, пов'язаних з уразливостями операційної системи й установленого програмного забезпечення.

Виявити уразливості вузла комп'ютерної мережі дозволяють сканери безпеки. Для більше точного й надійного визначення наявних уразливостей рекомендується використовувати два сканери безпеки від різних виробників, наприклад, MaxPatrol і Nessus. Усунути знайдені уразливості можна безпосередньо за допомогою деяких сканерів, служби Windows Update для локального вузла або спеціалізованого сервера – Windows Update Server для локальної мережі.

У свою чергу використання сканерів безпеки не дозволяє вирішити всі проблеми, з якими доводиться стикатися адміністраторам комп'ютерних мереж. Одна з таких проблем пов'язана з необхідністю забезпечення підключення до корпоративної мережі віддалених користувачів, які можуть працювати за публічними комп'ютерами вже зараженими вірусами. Тому наступним етапом розвитку засобів оцінки «здоров'я» вузлів комп'ютерної мережі є технологія NAC/NAP. Тепер у точці підключення комп'ютера до мережі виконується його комплексна перевірка й приймається рішення про можливий характер його доступу до мережі.

Протокол SCAP, розглянутий в кінці огляду, підтримується урядовими організаціями США і є відповіддю на погрози інформаційним системам з боку терористичних організацій. Завдання SCAP полягає в автоматизації процесу інформаційної безпеки, пропоновані рішення носять рекомендаційний характер і оформляються у вигляді спеціальних текстових файлів з відповідними параметрами безпеки. Для автоматизації процесу виконання перевірки провідними розробниками в області рішень інформаційної безпеки розроблені необхідні інструменти. На жаль, у даний момент інформація про характер їх використання й застосування відсутня.

Список літератури

1. *[Електрон. ресурс]. – Режим доступу: http://ko-online.com.ua/node/36686.*
2. *Элсенпитер Р. Microsoft Windows XP Professional. Администрирование сетей. Серия «Справочник администратора»: пер. с англ. / Р. Элсенпитер, Т.Дж. Велт. – М.: СП ЭКОМ, 2006. – 56с.*
3. *[Електрон. ресурс]. – Режим доступу: http://www.xakep.ru/post/47037/default.asp.*
4. *Лукацкий А.В. Обнаружение атак / А.В. Лукацкий – СПб.: БХВ – Петербург, 2003. – 624 с.*
5. *[Електрон. ресурс]. – Режим доступу: http:// www.itc.ua/2004/12/index.htm.*
6. *Мазулевський О.Є. Системи аналізу захищеності: сучасний стан і шляхи вдосконалення / О.Є. Мазулевський , С.В. Литвиненко // Інформаційні інфраструктура і технології. – 2007. – № 1. – С. 42-48.*
7. *Журнал «IT-спец» №12, 2007. Сканери безпеки.*
8. *[Електрон. ресурс]. – Режим доступу: http:// www.itsecurity.ru/news/reliase/2008/12_22_08.htm.*
9. *[Електрон. ресурс]. – Режим доступу: http://ko-online.com.ua/node/19351 WUS.*
10. *Журнал «IT-спец». – №05, 2007. NAC.*

11. [Електрон. ресурс]. – Режим доступу: http://www.pluscom.ru/index.php?option=com_content&task=view&id=505&Itemid=70.

12. [Електрон. ресурс]. – Режим доступу:http://ko-online.com.ua/node/35943.

13. Новое определение NAC. [Електрон. ресурс]. – Режим доступу: http://www.osp.ru/news/articles/2009/10/6591732/.

14. [Електрон. ресурс]. – Режим доступу: http://blogs.technet.com/stbgrus/archive/2008/02/06/2837766.aspx.

15. [Електрон. ресурс]. – Режим доступу:http://www. iso27000. ru/informacionnye-rubriki/ audit-informacionnoi-bezopasnosti/bazovye-konfiguracii-rabochih-stancii-dlya-federalnyh-agenstv-ssha.

Надійшла до редколегії 22.10.2009

Рецензент: д-р техн. наук, проф. О.Л. Ляхов, Полтавський національний технічний університет ім. Ю. Кондратюка, Полтава.

ОБЗОР СРЕДСТВ И ТЕХНОЛОГИЙ КОНТРОЛс УЗЛОВ КОМПЬЮТЕРНОЙ СЕТИ

А.Н. Юдин, П.Н. Гроза, С.В. Сомов, О.В. Тесленко

В статье рассмотрены средства оценки и настройки безопасности узлов компьютерной сети, поиска и устранения уязвимостей, а также технологии CISCO и Microsoft, позволяющие контролировать подключение удаленного компьютера к корпоративной сети.

Ключевые слова: *шаблоны безопасности, средства анализа защищенности, сканер безопасности, системы управления обновлениями, контроль доступа к корпоративной сети, протокол автоматизации управления данными безопасности.*

THE REVIEW OF THE CONTROL FACILITIES AND TECHNOLOGIES OF THE COMPUTER NETWORK'S UNITS

A.N. Yudin, P.N. Groza, S.V. Somov, O.V. Teslenko

Facilities of estimation and tuning of safety of knots of computer network, search and removal of vulnerable places, and also technologies of CISCO and Microsoft, allowing to control connecting of remote computer to the corporate network, are considered in the article.

Keywords: *templates of safety, facilities of analysis of protected, scintiscanner of safety, control system by updates, access control to the corporate network, protocol of automation of management of data of safety.*