УДК 004.7

АУДИТ МЕРЕЖЕВОГО ОБЛАДНАННЯ ВЕЛИКОГО ВИРОБНИЦТВА

Ковальська Д.Д., Курдеча В.В.
Інститут телекомунікаційних систем „КПІ ім. Ігоря Сікорського”
E-mail: zashkvar.youtuba01@gmail.com

AUDIT OF LARGE-SCALE NETWORK EQUIPMENT

Suggestions for improving the audit of a large network through the use of modern technologies, namely software.

Аудит як поняття у телекомунікаціях означає збір даних для аналізу та подальшої обробки, в основному, із ціллю удосконалення існуючої мережі. Це невід’ємна частина модернізації та перевірки поточного стану існуючої інфраструктури. Також це є обов’язковим етапом для перевірки стійкості мережі до зовнішніх загроз та тестування обладнання на стійкість до різних типів атак.

Разом із розвитком Інформаційних Технологій міняються і способи для ефективного проведення аудиту. Проте, під впливом значно швидшого оновлення *технічних і фізичних складових мережі* ріст є недостатнім і аудит так і лишається поняттям, котре описує у *більшому степені* фізичне втручання спеціаліста, яке потребує багато часу, унаслідок чого витрати можуть бути непомірно великими.

Ця стаття присвячена методам спрощення аудиту за допомогою програмного забезпечення та чіткому плану дій, котрий значно скоротить час на виявлення та усунення несправностей у роботі мережевого обладнання. Особливо актуальною дана стаття буде для великих виробництв, адже ефективність дорівнює не лише малій вартості, але й швидкому аналізу та модернізації, за рахунок чого не втратиться продуктивність роботи.

Для початку потрібно виділити основні моменти аудиту, на які варто орієнтуватись при плануванні:

1. Організаційно-технологічні особливості галузі та вплив мережевого обладнання на ефективну роботу
2. Визначення ряду програмного забезпечення для аудиту
3. Побудова логічної схеми інфраструктури
4. Виділення основних груп користувачів інфраструктури
5. Принципи побудови, мережеве ядро та схематичне зображення мережевої інфраструктури
6. Фізична та апаратна серверна інфраструктура – опис та візуалізація
7. Вивчення мережевих сервісів
8. Виявлення недоліків у мережі та їх опис
9. Рекомендації щодо виправлення недоліків та можливі варіанти їх усунення

Слідуючи плану, можна виділити деякі найбільш важливі пункти, які складають вагому частину аудиту (рис.1).

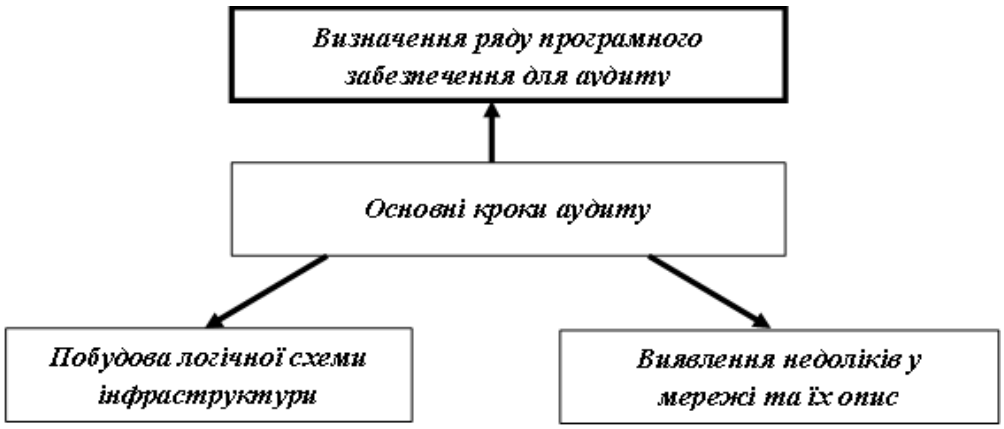

Рис.1. Основні кроки аудиту.

Усі ці пункти нараз можуть відобразити недостатню ефективність системи аудиту у реаліях сучасних мереж. Для прикладу, фізична складова, як можливість огляду і інвентаризації обладнання, застосовується набагато більше, ніж більш доскональне програмне забезпечення[1] (далі – ПЗ), котре має такі ж функції. Більше того, опитування та аналіз не позиціонується як інформація, котра потребує додаткової перевірки. За рахунок цього величина помилки людського фактору збільшується разом із часом проведення аудиту.

Застосовуючи ПЗ як основний метод аудиту, або додатковий (перевірковий), відсоток достовірності даних значно росте, що дозволяє правильно аналізувати та модернізувати мережу.

Для прикладу ми візьмемо велике виробництво.

Серверна інфраструктура скрадатиметься із:

- серверного обладнання;
- віртуальних машин;
- мережевого обладнання.

В середньому, слідуючи із мого досвіду і математичних розрахунків, виробництво із 100 серверами та віртуальними машинами буде потребувати близько 250 годин, що дорівнює 325 000 (триста двадцять п’ять тисячгривень)*, при звичному аудиту, без перевірки отриманих даних. Тому перед нами постає питання: «Як зменшити час і кошти на проведення аудиту мережі?».

В середньому, участь берутьщонайменше 3 спеціаліста: фахівець з інформаційної безпеки, фахівець з комп’ютерних мереж, інфраструктурний архітектор. Наше завдання – спробувати скоротити кількість працівників, та час їх безпосередньої участі. Задля цієї мети і застосовується ПЗ. Важливо зазначити, що ціллю не є повне виключення фізичного втручання в процеси аудиту, а лише його максимальне спрощення, без втрачання повноти і якості наданої інформації по головній цілі аудиту – визначенню вразливостей та плану їх запобігань, якщо цього потребує технічне завдання.

Вибір ПЗ базується, в основному, на кількості обладнання, що знаходиться всередині існуючої мережі, якщо ми беремо до прикладу велике виробництво, розрахунки на фізичний аудит якого навели вище, то середня ціна програмного забезпечення буде дорівнювати 27 000 (двадцяти семи тисячам гривень)*. Для розрахунку брались 4 найпопулярніші рішення (WhatsUpGold, FortiAnalyzeri т.д), з котрих ми шукали середнє значення. Варто бути уважними і вибрати ПЗ, виходячи із тих завдань, котрих потребує аудит. Це вирішує перший пункт плану із вибором програмного забезпечення.

В основному, мережеве програмне забезпечення створене задля того, щоб спростити шлях спілкування машин із спеціалістом до однієї машини-менеджера, котра повинна

видавати стан роботи машини та інші показники, котрі є важливими у безперебійній роботі. Проте, ще одним із завдань ПЗ зазвичай є інвентаризація обладнання, котра навіть при сучасному аудиті проводиться вручну із залученням фахівця із комп'ютерних мереж і побудова логічної схеми роботи. Якщо, з допомогою вищенаведених методів, автоматизувати даний процес, то ми значно скоротимо час фізичного втручання працівників і, як наслідок, час аудиту, що вирішить питання залучення інфраструктурного архітектора.

Виявлення недоліків мережі та їх опис має базуватись на зібраній інформації не лише від ПЗ, але й від наданої технічними працівниками даної установи, та складатись виключно із проміжку робочого часу (тобто активного часу роботи обладнання та серверної інфраструктури).Аудитор повинен використовувати отриману інформацію для визначення відповідної мети. Знайшовши безліч уразливостей, необхідно вибрати серед них ту, котра виявилась найбільш придатною для дослідів та найменш захищеною. Знайшовши, наприклад, безліч уразливих робочих станцій і кілька серверів, краще зосередити свою увагу на останніх, так як їх злом допоможе розвивати подальшу атаку більш ефективно. На мою думку, у цьому етапі спеціалісти мають приймати найбільш активну участь, адже виявлення вразливостей, по суті, і має бути головним завданням аудиту. Опис повинен проводитись зрозумілою мовою, без застосування специфічних технічних термінів, у відповідності до наданого на початку роботи технічного завдання. У даному питанні застосування ПЗ для спрощення роботи є мінімальним, воно потребується лише для звірення даних, котрі надані технічними спеціалістами та використання логічних схем та інвентаризації, метод якої описано вище.

За допомогою математичних розрахунків, можна зробити висновки що аудит став дешевшим, ефективнішим та продуктивнішим, за рахунок використання сучасних технологій. Тепер , виробництво із 100 серверами та віртуальними машинами буде потребувати близько 190 годин, що на 60 годин менше попереднього значення, і, як наслідок, всього 274 000 (двісті сімдесят чотири тисячі) витрат, що на 51 000 (п'ятдесят одну тисячу) менше розрахунків, проведених виключно із фізичним втручанням*, залучення всього двох спеціалістів: фахівця з інформаційної безпеки та фахівця з комп'ютерних мереж. Це стало можливим завдяки скорочення часу на інвентаризацію та побудову логічної схеми, що значно спростило і скоротило час роботи спеціалістів мережевого сегменту і зовсім мінімізувало завдання інфраструктурного архітектора.

Аудит – це процес, який повинен проаналізувати мережу на всі можливі вразливості, тому через занадто велику можливість людської помилки і була створена ця методологія, заякою можна побудувати план аудиту із застосуванням програмного забезпечення і значно скоротити час і ресурси на виконання цього завдання.

Отже, за висновками проведеного експериментального дослідження нам вдалось скоротити час аудиту на 24%, що свідчить про значні успіху у цьому напрямку. Для написання матеріалу використовувалась спеціально сконструйована мережа, котра складалась із віртуальних машин.

Література

1. Гаврилова Л.В., Ян ван Тайнен, Шкуропат О.Г., Манфред ван Кестерен, Герард ван ден Берг, Рудніцька Р.М.,Чорнуцький С.П., Тимохін М.Г., Боровкова Т.В., Любиш-Родченко А.Г., Горбачев С.В.//ПРАКТИЧНА МЕТОДОЛОГІЯ ІТ-АУДИТ.
2. Самойленко В.В. Локальные сети. Полноеруководство. — К., 2002. — ISBN 966-7140-28-8. Архивнаякопия от 11 января 2012 на WaybackMachine.