УДК 004.01:004.71:004.72:004.032

ПРОБЛЕМИ АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ

Ковальська Д.Д., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: darinakovalskaaa@gmail.com

PROBLEMS OF AUDITING THE INFORMATION COMMUNICATION NETWORK OF LARGE ENTERPRISES

Increasing informatization of society leads to the need for effective methods of creating, controlling and auditing information communication networks. The method of auditing the information communication network of large enterprises is an integral part of infrastructure management and its security. It includes the collection and analysis of data on the state of the network, checking its resistance to external threats, testing equipment for resistance to attacks and other important processes.

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. Метод аудиту інфокомунікаційної мережі великих підприємств є невід'ємною частиною управління інфраструктурою та її безпекою. Він включає в себе збір та аналіз даних про стан мережі, перевірку її стійкості до зовнішніх загроз, тестування обладнання на стійкість до атак та інші важливі процеси.

Модернізація методів аудиту інфокомунікаційної мережі є необхідною для забезпечення безперебійної роботи великих підприємств. Сучасні технології дозволяють автоматизувати процеси збору та обробки даних, що забезпечує високу достовірність результатів та скорочення часу на проведення аудиту. Крім того, використання програмного забезпечення дозволяє проводити інвентаризацію обладнання автоматично, що зменшує необхідність у фізичному втручанні спеціалістів і зменшує витрати на аудит.

При цьому, модернізація методів аудиту дозволяє підвищити рівень безпеки мережі та забезпечити стійкість до зовнішніх загроз. Таким чином, впровадження нових методів аудиту допоможе підприємствам ефективніше використовувати ресурси та зменшити ризики виникнення проблем в роботі мережі.

Однією з головних проблем, які можуть виникнути при аудиті мережі, є необхідність у великій кількості людських ресурсів та часі для збору та обробки даних про стан мережі. Крім того, традиційні методи аудиту можуть бути неефективними у виявленні нових загроз та уразливостей, що можуть виникати з часом.

Це може бути складним і затратним процесом для компаній, що не мають достатнього досвіду в галузі мережевої безпеки.

Однак, існує ряд нових технологій, які можуть допомогти вирішити ці проблеми. Наприклад, автоматизовані системи моніторингу та виявлення інцидентів можуть значно скоротити час на виявлення та реагування на проблеми в мережі. Штучний інтелект та машинне навчання також можуть бути використані для аналізу великої кількості даних та виявлення нових загроз та уразливостей.

Крім того, зростаюча популярність хмарних технологій та віртуалізації дозволяє компаніям зменшити кількість необхідних фізичних ресурсів та спростити управління мережею.

Використання сучасних технологій та програмного забезпечення може вирішити ці проблеми, дозволяючи автоматизувати процеси збору та обробки даних, а також проведення інвентаризації обладнання. Це забезпечує високу достовірність результатів та скорочення часу на проведення аудиту. Більше того, такий підхід може допомогти виявляти нові загрози та уразливості та вчасно їх усувати, що забезпечить високий рівень безпеки мережі.

Іншою важливою проблемою є зменшення витрат на аудит. Використання програмного забезпечення дозволяє проводити інвентаризацію обладнання автоматично, що зменшує необхідність у фізичному втручанні спеціалістів та зменшує витрати на аудит .Участь у управлінні мережею та її безпекою - регулярне проведення аудиту, який має бути виконаний професіоналами з відповідним досвідом та знаннями. Однак, з огляду на високу складність мереж та збільшення їх обсягу, ручне виконання аудиту стає все складнішим та часозатратним, а також не виключає можливість людської помилки. Тому, використання сучасних технологій та програмного забезпечення є надзвичайно важливим для оптимізації процесу аудиту та забезпечення ефективного управління мережею.

Наприклад, однією зі сучасних технологій, яка може бути використана для аудиту, є технологія "інтернету речей" (Internet of Things, IoT). Вона дозволяє підключати до мережі різні пристрої, які забезпечують збір та передачу даних про стан мережі. За допомогою аналізу цих даних можна виявляти вразливості та загрози, що дозволяє підвищити рівень безпеки мережі та запобігти виникненню проблем у роботі. На рис. 1 представлене реальне застосування програмного забезпечення Netdisco для мережевого аудиту великого виробництва, на рисунку представлений повний перелік усіх мережевих пристроїв та як вони з’єднані один з одним.

Netdisco застосовується для збору інформації щодо активних MAC-адрес із подальшим зберіганням у своїй базі даних. Дані збираються з використанням опитувань SNMP і DNS-запитів, отримання представлення – за допомогою Mason.

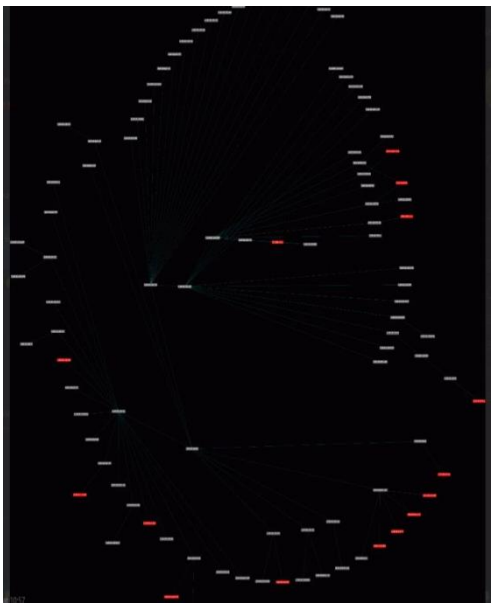

Рис. 1. Результат роботи ПЗ Netdisco.

У загальному, необхідно використовувати нові технології та інструменти для покращення ефективності аудиту мережі та забезпечення мережевої безпеки. Важливо також забезпечити постійне навчання та підвищення кваліфікації спеціалістів, що займаються мережевою безпекою, щоб вони могли ефективно використовувати нові технології та інструменти.

Отже, аналізуючи вище представлену інформацію, можна дійти висновку що спрощення аудиту і перехід від фізичного до аудиту із, у більшій мірі, застосуванням програмного забезпечення є можливим, і, більше того, необхідним.

Модернізація методів аудиту дозволяє ефективніше використовувати ресурси та зменшувати ризики виникнення проблем в роботі мережі. Використання сучасних технологій та програмного забезпечення забезпечує автоматизацію процесів збору та обробки даних, що забезпечує високу достовірність результатів та скорочення часу на проведення аудиту.

Однак, необхідно враховувати важливість постійного моніторингу мережі та вчасного виявлення нових загроз та уразливостей для забезпечення високого рівня безпеки мережі.

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 IT-АУДИТУ
2. Самойленко В.В. Локальні мережи. Повне керівництво. — К., 2002. — ISBN 966-7140-28-8. Архивна копія от 11 січня 2012 на Wayback Machine.