УДК 004.77

Шкурупій М.І.,
Дегтярьова Л.М., к.т.н., доцент
Полтавський національний технічний
університет імені Юрія Кондратюка

СИСТЕМИ ОЦІНКИ ІТ-ВРАЗЛИВОСТЕЙ ПРИ ОБРОБЦІ РЕЗУЛЬТАТІВ АУДИТУ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

***Анотація**. В даний час все більше актуальності на ринку інформаційної безпеки набуває послуга інформаційного аудиту. Дана стаття дає докладну класифікацію послуг і акцентує увагу на особливостях різних видів інформаційного аудиту. Крім того, наведено основні критерії оптимального вибору і застосування того чи іншого виду аудиту та його актуальності.*

***Ключові слова:** Інформаційна система, аудит безпеки, програмні засоби, ІТ-вразливості, захист інформації*

Вступ

Проблема захищеності корпоративних інформаційних систем сьогодні як ніколи актуальна. У ЗМІ постійно з'являються повідомлення про те, як найбільші компанії втрачають гроші і довіру партнерів через злам їхніх інформаційних систем. При цьому кожна з цих компаній вкладає, безумовно, чималі гроші в інформаційну безпеку. Однак захист інформації може бути досить дорогим, та неефективним: надійність захисту залежить не тільки від обсягу інвестицій, але і від того, як він організований.

Найпоширеніші причини зламу корпоративної інформаційної системи - це помилки веб-додатків, небезпечні бездротові мережі, помилки в налаштуваннях програмного забезпечення, програми, написані аутсорсерами (які можуть не

повідомляти про вразливість в розроблених ними додатках і навіть не знати про їх наявності).

Для ефективного захисту інформаційної системи компанії від небажаних проникнень, необхідна об'єктивна оцінка рівня безпеки інформаційної системи - саме для цих цілей і застосовується аудит безпеки.

Поняття інформаційного аудиту

На даний момент в інформаційній безпеці немає конкретного визначення інформаційного аудиту. Існує поняття, котре використовується фахівцями: Аудит інформаційної безпеки - системний процес отримання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки компанії відповідно до визначених критеріїв та показниками безпеки.

Таким чином, аудит в даному випадку зводиться до перевірки системи інформаційної безпеки та порівнянню результатів даної перевірки з певним ідеалом.

Активний аудит

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності інформаційної системи з точки зору хакера (або зловмисника, який володіє високою кваліфікацією в області інформаційних технологій). Компанії, що надають послуги активного аудиту називають його інструментальним аналізом захищеності, щоб відокремити даний вид аудиту від інших.

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення і спеціальних методів здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміються лише ті параметри і налаштування, використання яких допомагає хакеру проникнути в мережі і завдати шкоди компанії.

При здійсненні даного виду аудиту на систему мережевого захисту моделюється як можна більшу кількість таких мережевих атак, які може виконати хакер. При цьому аудитор штучно ставиться саме в ті умови, в яких працює хакер, - йому надається мінімум інформації, тільки та, яку можна роздобути в відкритих джерелах. Природно, атаки всього лише моделюються і не надають будь-якого деструктивного впливу на інформаційну систему. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора. Результатом активного аудиту є інформація про всі слабкі місця, ступеня їх критичності і методах усунення, відомості про широкодоступної інформації (інформація, доступна будь-якому потенційному порушнику) мережі замовника.

Після закінчення активного аудиту видаються рекомендації по модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливі місця і тим самим підвищити рівень захищеності інформаційної системи від дій зловмисника при мінімальних витратах на інформаційну безпеку.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту не можна зробити висновок про коректність, з точки зору безпеки, проекту інформаційної системи.

Активний аудит - послуга, яка може і повинна замовлятися періодично. Виконання активного аудиту, наприклад, раз на рік, дозволяє упевнитися, що рівень системи мережевої безпеки залишається на колишньому рівні.Активний аудит умовно можна розділити на два види: «зовнішній» активний аудит і «внутрішній» активний аудит.

При «зовнішньому» активному аудиті фахівці моделюють дії «зовнішнього» зловмисника. В даному випадку проводяться такі процедури:

- сканування даних IP-адрес замовниказ метою визначення працюючих сервісів і служб, відстеження призначення від сканованих хостів;

- визначення версій сервісів і служб сканованих хостів;
- вивчення маршрутів проходження трафіку до хостів замовника;
- збір інформації про замовника з відкритих джерел;
- аналіз отриманих даних з метою виявлення вразливостей.

«Внутрішній» активний аудит за складом робіт аналогічний «Зовнішньому», однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Іноді в ході активного аудиту замовнику пропонується ряд додаткових послуг, безпосередньо пов'язаних з оцінкою стану системи інформаційної безпеки, зокрема - проведення спеціалізованих досліджень.

Найчастіше організація в своїй інформаційній системі використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). ПодібнеПЗ унікальні, тому будь-яких готових засобів і технологій для аналізу захищеності і відмовостійкості даного ПЗ не існує. В даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Ще один вид послуг, пропонованих в ході активного аудиту, - дослідження продуктивності і стабільності системи, або стрес-тестування. Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні запити користувачів.Стрес-тест дозволить виявити «вузькі» місця в процесі формування та передачі інформації і визначити ті умови, при яких нормальна робота системи неможлива. Тестування включає в себе моделювання атак на відмову в обслуговуванні, призначених для користувача запитів до системи і загальний аналіз продуктивності.

Однією з найбільш «ефектних» послуг є тест на проникнення (PenetrationTesting), який багато в чому схожий на «зовнішній» активний аудит,

але по своїй суті аудитом не є.Основна мета даного тестування - демонстрація «успіхів», яких може досягти хакер, який діє при поточному стані системи мережевої захист. Результати даної послуги більш наочні, ніж результати аудиту. Однак їй властиві безліч обмежень і особливостей. Наприклад, особливість технічного характеру: замовник інформується тільки про факт вразливості системи мережевого захисту, в той час як в результатах «зовнішнього» активного аудиту замовнику повідомляється не тільки факт вразливості мережі, а й інформація про всі слабкі місця і способи їх усунення.

Експертний аудит

Експертний аудит можна умовно уявити, як порівняння стану інформаційної безпеки з «ідеальним» описом, котрий базується на наступному:

- вимоги, які були пред'явлені керівництвом в процесі проведення аудиту;
- опис «ідеальної» системи безпеки, засноване на акумульованому в компанії-аудитора світовому і приватному досвіді.

При виконанні експертного аудиту співробітники компанії-аудитора спільно з представниками замовника проводять такі види робіт:

- збір вихідних даних про інформаційну систему, про її функціях і особливостях, використовувані технології автоматизованої обробки і передачі даних (з урахуванням найближчих перспектив розвитку);
- збір інформації про наявні організаційно-розпорядчих документах щодо забезпечення інформаційної безпеки і їх аналіз;
- визначення точок відповідальності систем, пристроїв і серверів захисту;
- формування переліку підсистем кожного підрозділу компанії з категорією критичної інформації та схемами інформаційних потоків.

Один з найбільш об'ємних видів робіт, які проводяться при експертному аудиті, - збір даних про інформаційну систему шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.Основна мета інтерв'ювання технічних фахівців - збір інформації про функціонування мережі,

а керівного складу компанії - з'ясування вимог, які пред'являються до системи інформаційної безпеки. Необхідно відзначити, що при експертному аудиті безпеки інформаційної системи враховуються результати попередніх обстежень (в тому числі інших аудиторів), виконуються обробка і аналіз проектних рішень та інших робочих матеріалів, що стосуються питань створення інформаційної системи.

Ключовий етап експертного аудиту - аналіз проекту інформаційної системи, топології мережі та технології обробки інформації, в ході якого виявляються, наприклад, такі недоліки існуючої топології мережі, які знижують рівень захищеності інформаційної системи.За результатами робіт даного етапу пропонуються зміни (якщо вони потрібні) в існуючій інформаційній системі і технології обробки інформації, спрямовані на усунення виявлених недоліків з метою досягнення необхідного рівня інформаційної безпеки.

Наступний етап - аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків організації та складається їх діаграма, де для кожного інформаційного потоку вказується його цінність (в тому числі цінність переданої інформації) і використовувані методи забезпечення безпеки, що відображають рівень захищеності інформаційного потоку.На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент інформаційної системи, які беруть участь в найбільш важливих процесах передачі, зберігання і обробки інформації. Для менш цінної інформації рівень захищеності залишається колишнім, що дозволяє зберегти для кінцевого користувача простоту роботи з інформаційною системою.

В рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту та різного роду інструкції. Організаційно-розпорядчі документи оцінюються на предмет достовірностіта несуперечності декларованим цілям і заходам інформаційної безпеки. Особливу увагу на етапі аналізу інформаційних потоків приділяється

визначенню повноважень і відповідальності конкретних осіб за забезпечення інформаційної безпеки різних ділянок підсистем.

Результати експертного аудиту можуть містити різнопланові пропозиції щодо побудови або модернізації системи забезпечення інформаційної безпеки, наприклад:

- зміни (якщо вони потрібні) в існуючій топології мережі і технології обробки інформації;
- рекомендації по вибору і застосуванню систем захисту інформації та інших додаткових спеціальних технічних засобів;
- пропозиції щодо вдосконалення пакета організаційно-розпорядчих документів;
- пропозиції по етапах створення системи інформаційної безпеки;
- орієнтовні витрати на створення або вдосконалення інформаційної безпеки.

Аудит на відповідність стандартам

Суть даного виду аудиту найбільш наближена до тих формулювань і цілей, які існують у фінансовій сфері - при проведенні даного виду аудиту стан інформаційної безпеки порівнюється з якимсь абстрактним описом, що приводиться в стандартах.

Офіційний звіт, підготовлений в результаті проведення даного виду аудиту, включає наступну інформацію:

- ступінь відповідності перевіряється інформаційної системи обраним стандартам;
- ступінь відповідності власним внутрішнім вимогам компанії в області інформаційної безпеки;
- кількість і категорії отриманих невідповідностей і зауважень;

•рекомендації з побудови або модифікації системи забезпечення інформаційної безпеки, що дозволяють привести її у відповідність з даним стандартом;

•детальні посилання на основні документи замовника, включаючи політику безпеки, опису процедур забезпечення інформаційної безпеки, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються до даної компанії.

Нижче перераховані приклади стандартів, на відповідність яким проводиться аудит системи інформаційної безпеки:

•Міжнародний стандарт ISO / IEC 17799 «Інформаційні технології. Управління інформаційною безпекою »(InformationTechnology - InformationSecurityManagement). На сьогоднішній день є одним з найбільш поширених і широко застосовуваним стандартом у всьому світі.

•Міжнародний стандарт WebTrust. Застосуємо для підтвердження високого рівня захищеності системи електронної комерції і web-сервісів.

Причини проведення аудиту на відповідність стандарту (і сертифікації) можна умовно розділити за ступенем обов'язковості даної послуги по відношенню до компанії: обов'язкова сертифікація; сертифікація, викликана «зовнішніми» об'єктивними причинами; сертифікація, що дозволяє отримати вигоди в довгостроковій перспективі; добровільна сертифікація. Державні організації, які обробляють відомості, що становлять державну таємницю, відповідно до законодавства зобов'язані проводити атестацію інформаційної системи (багато в чому процедура аналогічна сертифікації). Однак такі організації найчастіше користуються не послугою аудиту на відповідність стандартам, а в обов'язковому порядку проводять атестацію власних інформаційних систем за участю атестаційних центрів.

Висновок

На закінчення відзначимо, що при плануванні перевірки стану системи інформаційної безпеки важливо не тільки точно вибрати вид аудиту, виходячи з потреб і можливостей компанії, але й не помилитися з вибором виконавця. Результати будь-якого виду аудиту повинні містити рекомендації з модернізації системи забезпечення інформаційної безпеки. Звіт по аудиту IT-інфраструктури повинен давати оцінку загального стану IT-інфраструктури (кількісного і якісного), проблемних і «вузьких» місць, список рекомендацій по їх усуненню, результати дослідження апаратної і програмної складових інфраструктури та оцінку їх надійності, а також рекомендації щодо поліпшення інфраструктури і по виправленню виявлених помилок.

Література

1. Васильцов, І.В. Класифікація сучасних атак спеціального виду на реалізацію / І.В. Васильцов, Л.О. Дубчак // Захист інформації. — 2007. — № 4. — С. 10–21.

2. Scarfone Karen. Guide to Intrusion Detection and Prevention Systems (IDPS) – 2007. – 127 p.

3. Mattord Verma. Principles of Information Security – 2008. – 300 p.

4. Sen Sevil. Power-Aware Intrusion Detection in Mo- bile Ad Hoc Networks – 2006. – 20 p.

5. Anderson Ross. Security Engineering: A Guide to Building Dependable Distributed Systems – 2007. – 388 p.

6. Jackson Kathleen. A Phased Approach to Network Intrusion Detection – 1991. – 30 p.

7. Syngress. Snort IDS and IPS Toolkit – 2007. – 197 p.

8. ДСТСЗІ СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несан- кціонованого доступу» — 2003. — 16 с.

9. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем — 2009. — 608 с.

Authors:
L. Degtyaryova, M Shkurupii

SYSTEMS FOR ASSESSING IT VULNERABILITY WHEN PROCESSING THE RESULTS OF CORPORATE NETWORK SECURITY CONTROL

Abstract. Currently, the information control service is becoming increasingly relevant in the information security market. This article gives a detailed classification of services and focuses on

the peculiarities of various types of information control. In addition, the main criteria for the optimal choice and application of this or that type of controls and its relevance.

Keywords: Information system, security audit, software tools, IT vulnerabilities, information security.

Авторы:
Дегтярьова Л.М., Шкурупий М.И.

СИСТЕМЫ ОЦЕНКИ ИТ-УЯЗВИМОСТИ ПРИ ОБРАБОТКЕ РЕЗУЛЬТАТОВ АУДИТА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

Аннотация. В настоящее время все больше актуальности на рынке информационной безопасности приобретает услуга информационного аудита. Данная статья дает подробную классификацию услуг и акцентирует внимание на особенностях различных видов информационного аудита. Кроме того, приведены основные критерии оптимального выбора и применения того или иного вида аудита и его актуальность.

Ключевые слова: Информационная система, аудит безопасности, программные средства, ИТ-уязвимости, защита информации.