УДК 004.056

О.О. Будік

Національний університет «Львівська політехніка», Львів

ВИБІР МЕТОДУ РАНЖИРУВАННЯ ВРАЗЛИВОСТЕЙ ДЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Розглянуто відомі підходи до ранжирування вразливостей та запропоновано вибір одного з них для ранжирування вразливостей в інформаційній системі вищого навчального закладу.

Ключові слова: *ранжирування вразливостей, інформаційна система, вищий навчальний заклад.*

Вступ

На жаль, часто бюджет, що виділяється на забезпечення ІБ, є досить обмежений. Згідно дослідження 2006 CSI/FBI, більше 47% компаній, що входять у список Fortune 500, витрачають лише 2% чи менше зі свого сукупного бюджету на безпеку. Зважаючи на обмеженість ресурсів, необхідно оптимально витрачати їх на ІБ. І одним із завдань вирішення цієї складної комплексної задачі є пріоритетизація загроз безпеці і вразливостей відповідно до особливостей діяльності організації.

Метою цієї роботи є окреслення відомих підходів до ранжирування вразливостей та вибір серед них оптимального для інформаційної системи вищого навчального закладу.

1. Інформаційна система ВНЗ та її особливості

ІС ВНЗ – організаційно-технічна система, в котрій реалізуються інформаційні технології, і передбачається використання апаратного і програмного забезпечення, необхідного для реалізації процесів збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформації

До ключових особливостей ІС ВНЗ віднесемо:

широке впровадження засобів обчислювальної техніки у всі сфери навчального процесу та наукових досліджень, а також управлінські структури;

величезні об’єми інформації, що циркулюють у вищому учбовому закладі;

територіальна рознесеність окремих об’єктів як у місті, так і між філіалами і представництвами у інших містах;

використання сучасних інформаційних технологій, включаючи електронний документообіг, засоби телекомунікацій, розподілені бази даних, інтернет-технології;

розвиток різноманітних форм дистанційного навчання із використанням інформаційних технологій;

циркуляція та збереження інформації, що пов’язана з інтелектуальною власністю, методичне забезпечення учбового процесу.

2. Відомі підходи до ранжирування вразливостей

Система ранжирування вразливостей Microsoft Severity Rating System є однією з найпростіших і не вимагає від користувача розуміння процесу утворення рейтингу вразливості. Вона передбачає лише чотири рейтинги вразливості: критична, важлива, середня та низька. Ці рейтинги визначаються компанією Microsoft.

В одному з підходів на основі стандарту ISO:17799-00 вважається, що всі вразливості мають різний ступінь небезпеки $K_{неб}$, котрий можна кількісно оцінити, застосувавши до них операцію ранжирування.

Коефіцієнт небезпеки $K_{неб}$ для окремої вразливості можна визначити як відношення добутку усіх вищенаведених показників до максимального значення:

$$K_{неб} = \frac{K_1 K_2 K_3}{125}. \qquad (1)$$

Кожний показник оцінюється експертно-аналітичним методом по п’ятибальній системі. Причому, 1 відповідає найменшому ступеню впливу оцінюваного показника на небезпеку використання вразливості, а 5 – найбільшому.

Свою методику ранжирування вразливостей пропонує організація US-CERT. Вона передбачає два типи документів: Нотатки про вразливості (Vulnerability Notes), які в загальному описують вразливості незалежно від конкретного виробника, і документація від виробників (Vendor Information documents), яка дає інформацію про специфічне вирішення проблеми від постачальника програмного забезпечення. В системі ранжирування US-CERT значення метрики може знаходитися в межах від 0 до 180.

В 2001 році компанія nCircle вивела рейтингову формулу для ранжирування вразливостей, яка з тих пір не змінювалася і досі використовується в обчис-

леннях при визначенні ризиків в організаціях, які прийняли в якості стандарту для управління ІБ nCircle IP360.

Модель оцінки вразливостей IP360, її математична структура і змінні, були розроблені на основі багаторічного досвіду компанії nCircle з використанням даних, зібраних з декількох тисяч аудитів інформаційної безпеки. Первинними компонентами оцінки вразливості є:

t_n – кількість днів, що минули з часу публікації інформації про вразливість в більшості джерел;

r_n – фактор "клас ризику", який представляє здатність вразливості n проявлятися на системі типу s;

s_n – міра "набору знань і вмінь", які необхідні зловмиснику для успішного проведення атаки на хост з використанням вразливості n.

Оцінка вразливості проводиться за наступною формулою:

$$V_n = \sqrt{t_n} \times \frac{r_n!}{s_n^2}. \qquad (2)$$

Система ранжирування вразливостей Common Vulnerability Scoring System. Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS) – це відкрита схема, яка дозволяє обмінюватися інформацією про вразливості в інформаційних системах. CVSS складається з трьох метрик: базова метрика, часова метрика, контекстна метрика. Кожна метрика являє собою число (оцінку) в інтервалі від 0 до 10 і вектор – короткий текстовий опис із значеннями, які використовуються для виводу оцінки. Базова метрика відображає основні характеристики вразливості. Часова метрика відповідає таким характеристикам вразливості, котрі змінюються з часом, а контекстна метрика – характеристикам, які унікальні для середовища користувача.

Вектор уособлює собою відкриту архітектуру системи. Вектор – це текстова стрічка, котра містить значення, пов'язані із кожною метрикою. Вектор використовується для того, щоб точно відобразити, як була отримана оцінка.

3. Вибір системи ранжирування вразливостей для ІС ВНЗ

3.1. Формулювання вимог до системи ранжирування вразливостей. Так як для управління інформаційною безпекою у вищих навчальних закладах зазвичай залучаються спеціалісти, чия освіта мало пов'язана або зовсім не пов'язана із захистом інформації, то система ранжирування вразливостей має бути зрозумілою, достатньо легкою у використанні. При цьому, враховуючи гетерогенну структуру інформаційної системи вищого навчального закладу, велику кількість хостів та інші її особливості розглянуті вище, виділимо наступні вагомі критерії:

Врахування при оцінці вразливості цінності інформаційного ресурсу, що досліджується;

Врахування динамічної характеристики вразливості;

Можливість зведення до мінімуму необхідності використання експертних оцінок та ручної роботи при підрахунку оцінок вразливостей;

Вартість та доступність інструментальних засобів, необхідних для забезпечення процесу ранжирування вразливостей.

3.2. Вибір системи ранжирування вразливостей. Вимогам, сформульованим у п. 3.1, відповідають лише дві із розглянутих вище систем ранжирування вразливостей – nCircle та Common Vulnerability Scoring System. Обидва підходи враховують потенційні збитки в залежності від цінності ресурсу при можливій реалізації вразливості, зміну небезпеки вразливості з часом. Для порівняння характеристик цих систем, побудуємо наступну табл. 1.

Таблиця 1

Порівняльні характеристики CVSS та nCircle

Назва системи	CVSS	nCircle
Стандартизовані оцінки	Так	Ні
Вартість програмних інструментів	Є безкоштовні	Тільки платні
Можливості вибору інструментів	Широкі	Тільки ті інструменти, які пропонує компанія-розробник
Відкритість системи	Відкрита	Закрита
Документація	Добре документована	Добре документована
Вимоги до спеціальних знань у користувача	Низькі	Низькі

Отже, CVSS має більше переваг порівняно з nCircle. Такі її переваги, як наявність безкоштовних програмних інструментів, їх широкий вибір, зумовлені широкою розповсюдженістю цієї системи. Відкритість системи дозволяє кінцевому користувачу розуміти, яким чином була отримана оцінка вразливості. Вагомою перевагою є стандартизовані оцінки. Після нормалізації оцінок вразливостей для всіх програмних і апаратних платформ вищого навчального закладу може використовуватися єдина політика управління вразливостями, а це важливо з урахуванням складності структури ІС ВНЗ.

Висновки

У роботі подано короткий огляд найпоширеніших підходів до ранжирування вразливостей. Сформульованим до них вимогам з урахуванням особливостей інформаційних систем вищих навчальних закладів відповідають лише дві із розглянутих систем ранжирування вразливостей – nCircle та Common Vulnerability Scoring System. Врахувавши недоліки та переваги цих двох систем, приходимо до висновку, що доцільним є використання саме CVSS.

Розробка методології застосування CVSS для ранжирування вразливостей інформаційної системи вищого навчального закладу та оцінка її ефективності можуть бути предметами подальших наукових досліджень.

Надійшла до редколегії 30.03.2010

Рецензент: д-р техн. наук, доцент О.В. Потій, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ВЫБОР МЕТОДА РАНЖИРОВАНИЯ ЧУВСТВИТЕЛЬНОСТИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

А.А. Будик

Рассмотрены известные подходы к ранжированию чувствительности и предложен выбор одного из них для ранжирования чувствительности в информационной системе высшего учебного заведения.

Ключевые слова: *ранжирование чувствительности, информационная система, высшее учебное заведение.*

CHOICE OF METHOD OF RANGING OF SENSITIVENESS FOR THE INFORMATIVE SYSTEM OF HIGHER EDUCATIONAL ESTABLISHMENT

O.O. Budik

The known approaches are considered to ranging of sensitiveness and the choice of one of them is offered for ranging of sensitiveness in the informative system of higher educational establishment.

Keywords: *ranging of sensitiveness, informative system, higher educational establishment.*