**Чайковська М.П.**
доцент кафедри менеджменту та математичного моделювання ринкових процесів, к.е.н., доцент
**Азеев А.С.**
Одеський національний університет імені І.І. Мечникова

# ПИТАННЯ УПРАВЛІННЯ ЯКІСТЮ СИСТЕМИ БЕЗПЕКИ WEB-ДОДАТКІВ

Початок XXI століття характеризується швидкими темпами розвитку Інтернет, поширенням її впливу на життя суспільства. Згідно зі Internet World Stats [1], у світі налічується 2,5 млрд. користувачів, а з урахуванням підключення до Інтернету мобільних телефонів їх кількість зростає. Переміщення в Інтернет багатьох видів економічної діяльності стало підставою для створення віртуальних підприємств. Мережа Інтернет змінила попит, розширила пропозицію, залучила користувача у виробництво, дозволила його персоніфікувати, враховувати побажання, виробляти товари на замовлення. Розвиток Інтернет трансформує інструменти маркетингових комунікацій на базі інтерактивності, персоніфікації, гіпермедійності, аналітичності, таргетинговості [2, с. 205]. Інтернет став фактором і простором розвитку підприємництва, але створила нові ризики.

Метою дослідження є аналіз сучасних інформаційних загроз мережі Інтернет, з'ясуванні особливостей захисту в реаліях українського ринку, розробці рекомендацій щодо забезпечення якості системи безпеки на базі логіко-структурного підходу [3, с. 22].

Розробка нових web-додатків часто фокусується на досвіді замовника й найчастіше зводиться до забезпечення необхідної функціональності та якісного інтерфейсу. Увага приділяється й системі серверної інтеграції додатків. Багаторічний досвід різних компаній показує, що забезпечення якості системи безпеки web-додатків повинне починатися ще на ранніх стадіях процесу проектування й розробки додатків.

Метою вирішення проблем якості системи безпеки web-додатків, є: забезпечення високої доступності додатків, якість серверних рішень і захист конфіденційних даних, забезпечення розробки надійних і безпечних програмних рішень. Можливі різноманітні втрати – від простого блокування роботи сервера до заміни його змісту кримінальними матеріалами, політичними гаслами або видалення груп файлів, а також розміщення на сервері програм-троянів коней - значно впливають на показники якості системи безпеки web-додатків. Необхідно забезпечити можливість використання додатка одночасно

більшою кількістю відвідувачів. Продуктивність додатка не повинна падати в міру зростання навантаження на інтернет-ресурс. Це досягається використанням технології одержання інформації запитами та дозволяє сформувати комплекс рекомендацій щодо забезпечення якості системи безпеки web-додатків.

1. Розмістити веб-сервер у демілітаризованій зоні (DMZ). Зконфігурувати свій міжмережевий екран (файрволл) таким чином, щоб він блокував вхідні з'єднання з нашим веб-сервером з усіма портами, окрім http (порт 80) або https (порт 443).
2. Вилучити всі непотрібні сервіси з нашого веб-сервера, залишивши FTP та засіб безпечного підключення в режимі віддаленого терміналу, таке як SSH. Будь-який непотрібний, але залишений сервіс може стати помічником хакера при організації ним атаки.
3. Відключити всі засоби віддаленого адміністрування, якщо вони не використовують шифрування всіх даних сеансів або одноразових паролів.
4. Обмежити число людей, що мають повноваження адміністратора або суперкористувача (root).
5. Вести протокол усіх діх користувачів і зберігати системні журнали або в зашифрованій формі на веб-сервері, або на іншій машині в інтранеті.
6. Проводити регулярні перевірки системних журналів на предмет виявлення підозрілої активності. Встановити декілька програм-пасток для виявлення фактів атак сервера (наприклад, пастку для виявлення Phf-Атаки).
7. Вилучити всі непотрібні файли, такі як phf, з директорій, звідки можуть запускатися скріпти (наприклад, з /cgi-bin).
8. Вилучити всі стандартні директорії з документами, які поставляються з веб-серверами, такими як IIS і Exair.
9. Встановлювати всі необхідні виправлення програм на веб-сервері, що стосуються безпеки, як тільки про них стає відомо.
10. Якщо використовується графічний інтерфейс на консолі адміністратора веб-сервера, необхідно вилучити команди, які автоматично запускають його за допомогою інформації в. Rc-піддиректоріях і замість цього створити команду для його ручного запуску. По можливості залишати графічний інтерфейс працюючим тривалий період часу.
11. Для віддаленого адміністрування використовується програма, що встановлює захищене з'єднання з веб-сервером (наприклад, SSH). Не дозволяти встановлювати з веб-сервером telnet-з'єднання або неанонімні ftp-з'єднання (тобто ті, потребують введення імені й пароля) з недовіренних машин. Надати можливість встановлення таких з'єднань лише невеликому числу захищених машин, які перебувають в інтранеті.

12. Запускати веб-сервер в chroot-режимі або режимі ізольованої директорії, щоб не можна було одержати доступ до системних файлів.

13. Проводити всі оновлення документів на публічному сервері з інтранету. Зберігати оригінали веб-сторінок на веб-сервері в інтранеті й спочатку оновлювати їх на цьому внутрішньому сервері; потім копіювати оновлені веб-сторінки на публічний сервер за допомогою Ssl-з'єднання.

14. Періодичне сканування веб-серверу такими засобами, як ISS або nmap, для перевірки відсутності на ньому відомих уразливих місць.

15. Організувати спостереження за з'єднаннями із сервером за допомогою програми виявлення атак (intrusion detection).

Таким чином, управління якістю системи безпеки роботи веб-представництва й захисту інформації можливо тільки при постійному дотриманні комплексних захисних заходів. Безпека охоплює дуже широке коло проблем і змушує стежити за самими останніми новинками в цій області. Систему безпеки потрібно постійно підтримувати, її не можливо просто додати до проекту після того, як він завершений.

*Література:*

*1. Internet World Stats:[Електроний ресурс]. Режим доступу: www.internetworldstats.com/stats.htm;*

*2. Чайковська М.П. Перспективи гипермедійної інтеграції CR-систем / М.П. Чайковська // Економічний вісник університету. Збірник наукових праць. Вип. 18/2.- Переяслав-Хмельницький: П-Х ДПУ імені Г.Сковороди, 2012. - с.201-207.*

*3. Чайковська М.П. Проектування системи інформаційної безпеки на базі ЛСП/ А.С. Азеев, М.П. Чайковська // Економіка та управління в умовах побудови інформаційного суспільства. Матеріали ІІІ Міжнародної науково-практичної конференції. Том 2. - Одеса: ОНАЗ, 2014. - С.22-27.*