УДК 004.056.57 + 004.492

Є.А. Олійник

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО:ЗАХИЩЕНІСТЬ САЙТІВ ЗМІ

Вінницький національний технічний університет

Анотація

В даній роботі описуються вплив та роль ЗМІ в інформаційних війнах, їх місце в мережі інтернет та знайдено статистичні дані щодо найбільших вразливостей сайтів ЗМІ. Також було надано рекомендації щодо покращення рівня інформаційної безпеки.

Ключові слова: Інформаційне протиборство, ЗМІ, вразливості,інформаційна безпека.

Abstract

In the present research work describes the influence and role of the media in information wars, their place on the Internet, and finds statistics on the most vulnerable media sites. Also, recommendations were made to improve the level of information security.

Keywords: Information confrontation, media, vulnerabilities, information security.

Вступ

Інформаційні війни стали одним з найнебезпечніших видів зброї. Користуватися компроматами, виливанням бруду, підкиданням неправдивої інформації, намагання за допомогою інформації ввести в оману, стало для розповсюдженими методами впливу на соціум. Інформація має вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети: знищити опонента, прибрати з дороги конкурентів чи розпалити війну.

Журналісти тримають у руках зброю, тільки не завжди використовують її за призначенням. На тлі останніх подій, які відбуваються в Україні можна зрозуміти, що основна боротьба між політичними силами відбувається за допомогою інформації, тобто в країні почалося інформаційне протиборство.

Метою наукової роботи є дослідження впливу ЗМІ в мережі інтернет та захищеність сайтів від вторгнення[1].

Для досягнення мети необхідно розв’язати такі задачі:

- проаналізувати найбільш вразливі ресурси в мережі;
- здійснити пошук статистичних даних щодо вразливостей сайтів ЗМІ;
- надати рекомендації щодо підвищення рівня захисту сайтів.

Результати дослідження

Інформація - дуже широке поняття і включає в себе всі сфери людської діяльності та являє собою ресурс, яким оперує суб'єкт в процесі прийняття рішень зокрема в інформаційному протиборстві. Інфрмаційне протиборство передбачає якусь боротьбу в рамках будь-якої мети.

Атаки на сайти - вчинення протиправних дій щодо веб-сайтів спрямованих на отримання конкурентних переваг шляхом злому, зараження шкідливими кодом, блокування доступу (з подальшою вимогою викупу), крадіжку конфіденційних даних, виведення з ладу програмного забезпечення. Веб-сайти - це інформаційний актив і вид власності. Він може піддаватися атакам зловмисників з різними цілями. Сайт завжди на виду, завжди повинен бути доступний і це робить його вкрай вразливим[2].

За статистикою найчастіше атакують:

- платіжні системи;
- інформаційні агрегатори;
- електронна комерція;
- ігри та ігрові площадки;
- інші.

Веб-сторінки банків і електронних платіжних систем зламують з метою крадіжки грошей, сайти комерційних компаній ламають заради клієнтської бази і створення проблем конкуренту, або шантажу, вимагаючи гроші за відновлення нормальної роботи, сайти урядових органів і громадських організацій атакуються ідеологічними противниками.

У інформаційному протиборстві сайти ЗМІ мають досить великий вплив так як на великій кількості сайтів відображається стрічка новин. Саме таку інформації сприймають користувачі мережі і тому важливо забезпечити захист цих сайтів від можливості взлому їх зловмисником та подальшим використанням їх у своїх корисних цілях.

Згідно з дослідженням компанії Positive Technologies було виявлено, що саме сайти ЗМІ є найбільш вразливими до хакерських атак[3].

Всього в ході тестів з аналізу захищеності було вивчено близько 500 веб-сайтів, для 61 з них проводився поглиблений аналіз на наявність вразливостей. Досліджувалися сайти банків, ЗМІ, державних установ, промислових підприємств і телекомунікаційних компаній.

Виявилося, що у 62 відсотків сайтів були уразливості високого ступеня ризику з точки зору можливості несанкціонованого втручання в їх роботу. Це істотно більше, ніж було зазначено в попередньому дослідженні, проведеному в 2012 році, коли цей показник склав 45 відсотків.

Найбільше додатків з уразливостями високого ступеня ризику було виявлено на сайтах ЗМІ - 80 відсотків.

Що стосується сайтів дистанційного банківського обслуговування, то жодна з досліджених фінансових інтернет-систем не відповідала повністю вимогами стандарту безпеки даних індустрії платіжних карт (Payment Card Industry Data Security Standard, PCI DSS).

Найпоширеніша вразливість - міжсайтового виконання сценаріїв (Cross Site Scripting) - зустрічається на 78 відсотках досліджених сайтів. Ця вразливість дозволяє атакуючому впливати на вміст веб-сторінки, яка відображається в браузері користувача, в тому числі з метою поширення шкідливого коду або отримання облікових даних жертви.

На другому місці за поширеністю виявився слабкий захист від підбору ідентифікаторів або паролів користувачів.

Залежно від використаного мови програмування, застосованого для створення сайту, найнебезпечнішими виявилися сайти на основі мови PHP: 76% з них містять небезпечні уразливості. Кілька більш захищені веб-сайти на основі Java (70% з уразливими) і ASP.NET (55%).

Відповідно до виявлених загроз було розроблено рекомендації як покращити захист сайтів[4].

1. В багатьох випадках сайти конструюють не повністю з нуля, використовують готову систему управління сайтом. Для сайту ЗМІ варто повністю створювати нову систему управління сайтом, що не дасть використати зловмиснику типові вразливості CMS.
2. Ретельно перевіряти джерела скріптів які будуть використовуватись на сайті.
3. Контроль того, що вводить користувач на сайті через будь яку із форм.
4. Регулярно змінювати пароль(пароль повинен бути стійким великої довжини не менше 30 символів і включати в себе різні символи), саме через слабкі паролі відбувається багато атак.
5. Не зберігати паролі в панелі браузера або FTP клієнті.
6. Дозволити доступ до хостингу лише із свого IP.
7. Виставити в правах користувача правило «білого списку»(що не дозволено те не заборонено)

Користуючись лише цим набором правил можливість отримання несанкціонованого доступу до сайту стане набагато нижчою. І ризики, що ворог зможе використати аудиторію сайту у своїх інтересах стануть мінімізованими.

Висновки

В результаті аналізу статистичних даних було визначено, що найбільш популярною ціллю були саме сайти ЗМІ. Було проаналізовано найбільш часто використовуванні методи атак на ці сайти та на їх основі складено рекомендації, використавши які кількість сайтів які були взламані може скоротитись у декілька разів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи/ Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.

2. Атака на сайти[Електронний ресурс]. –Режим доступу: URL: https://www.anti-malware.ru/threats/websites-attacks/– Назва з екрану.

3. Статистика вразливостей веб-додатків в 2018 році[Електронний ресурс]. –Режим доступу: URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-vulnerabilities-statistics-2019/– Назва з екрану.

4. Як підвищити безпеку сайту і захистити його від взломів? [Електронний ресурс]. –Режим доступу: URL: https://www.site2b.com.ua/web-blog/zachem-nuzhna-povyshennaya-bezopasnost-sajta.html– Назва з екрану.

Олійник Євген Анатолійович **–** студент факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет.

Науковий керівник: ***Дудатьєв Андрій Веніамінович***– канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Oliynyk Yevgeny Anatolyevich- student of the Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University.

Supervisor: ***Dudatyev Andriy Veniaminovich***– Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine.