УДК 334.72

М. А. Томчук
С. А. Риндін

Значення безпеки інформаційних систем та програмного забезпечення під час використання кіберпростору

Вінницький національний технічний університет

Анотація: *В статті розглянуто значення безпеки інформаційних систем та ПЗ, загрози безпеки інформації, крадіжки персональних даних, а також відомі хакерські атаки та поради як уникнути кібератак.*
Ключові слова: безпека інформації, комп'ютерний вірус, веб-безпека, Stuxnet, вразливість, алгоритми безпеки.

Significance of information systems and software security when using cyberspace

Abstract: *The article considers the importance of information systems security and software, the of information security threat, personal data theft, and also well - known hacker attacks and tips how to avoid cyberattacks.*
Keywords: information security, computer virus, web security, Stuxnet, impressionability, security algorithms.

Сьогодні вже неможливо уявити своє життя без персонального комп'ютера. В даний час процес інформатизації проявляється у всіх сферах людської діяльності. Кожен, скільки б йому не було років, може зайти додому і вільно скористатися стандартним пакетом послуг, які встановлені на будь-якому комп'ютері.

Безпека інформаційних систем - це поняття, яке вказує на захищеність системи від навмисного чи випадкового втручання в процес її роботи, від спроб модифікації чи фізичного руйнування її компонентів, також від спроб несанкціонованого отримання інформації, тобто здатність протидіяти загрозам різного характеру.

Загроза безпеки інформації - це події або дії, які призводять до руйнування інформаційних ресурсів, несанкціонованого використання отриманої інформації, заміна даних керованої системи, а також програмних і апаратних засобів.

Загрози безпеки інформації поділяються на ненавмисні тобто випадкові і навмисні [1]. Вихід з ладу апаратних чи програмних засобів, неправильні дії користувачів чи працівників інформаційної системи, помилки в самому програмному забезпеченні - це все являється джерелом випадкових загроз. Такі загрози ненавмисні і не містять мету отримати вигоду. Навмисні загрози - це випадок коли існує мета нанесення шкоди конкретній системі чи користувачу. Зазвичай це робиться заради отримання певної особистої вигоди.

Найбільшою загрозою інформаційних систем є комп'ютерні віруси. Комп'ютерні віруси - це програми, які здатні до прихованого самопоширення та знищення або передачі інформації її розробникам. Жертвами вірусів стають не тільки звичайні користувачі, але ще й великі компанії та заводи і підприємства.

Так 2014 році відбулась атака на Sony Pictures, тоді у мережу потрапили сценарій Вінса Гіллігана (творець Breaking Bad) і кілька фільмів. Їх якість була невисока - це були промо-копії «Енні», «Люті», «Вільяма Тернера», «Все ще Еліс» і «Написати любов на її руках». Деякі фільми до моменту витоку ще не вийшли в прокат [2].

Інший відомий випадок це комп'ютерний червяк Stuxnet, який для звичайних користувачів не був небезпечний, вони були просто переносниками вірусу, він спав на їх пристроях, але потрапляючи на промислові контролери simatic S7 прокидався і починав диверсію. Так на заводі зі збагачення урану в Ірані вийшли з ладу понад 1000 центрифуг, вони повинні були обертаючись розділяти ізотопи урану, але після зараження розігнались до такої швидкості, що просто розлетілись. Іранська ядерна програма була відкинута на кілька років назад [3].

Але на цьому історія потужної кібератаки не закінчується. Справа в тому, що дістатися до обладнання на заводі було неможливо, воно не було підключено до інтернету та було захищено так, що навіть при ядерному вибуху завод зберігся б і нічого не постраждало б.

Обладнання було зламано офлайн, спочатку хакери заразили комп'ютера 5 компаній які поставляли обладнання для цього заводу, вірус поширювався і по теорії ймовірностей рано чи пізно хтось із співробітників приніс на зараженому флеш накопичувачі вірус, безпосередньо в контролер центрифуг.

Тобто черв'як гуляв по всьому світу, нічого не робив, півроку-рік, він чекав поки попаде в потрібне обладнання і як тільки потрапляв, прокидався, і так як він знав кожну операційну систему перевіряв кожен пристрій на який потрапляв, щоб зрозуміти як близько він знаходиться до мети.

Проте розробники антивірусів теж не стоять на місці, нині в лабораторіях існують спеціальні віртуальні машини на яких запускають віруси і дивляться, що робить код програми. Наприклад програма починає збирати різні паролі, міняти початкову сторінку браузера, скачувати і встановлювати стороні програми, вмикати камеру і шпигувати за користувачем. Вірус думає що це справжній комп'ютер і таким чином ловиться на гарячому, а все що він натворив спокійно відкатується. Самі розумні віруси розуміють, що вони знаходяться не в справжніх комп'ютерах, тоді доводиться імітувати рух мишею, натискання на клавіатуру, щоб було реалістично, все це відбувається віртуально. Таким же чином розробляється захист для заводів від таких вірусів як Stuxnet.

Розробляються спеціальні алгоритми, які слідкують за виробництвом і бачать коли відбувається якась аномалія, наприклад десь збільшився тиск чи центрифуги дуже швидко крутяться. І якщо виявлена проблема то повідомляється працівнику.

Поради по безпеці користувачам:

1. Обов'язково видаляйте знімки екрану повідомлень де є паролі.
2. Не зберігайте паролі в браузері.
3. Не завантажуйте неперевірені файли, документи, вкладення чи додатки. Не натискайте на невідомі посилання, оголошення, сайти.
4. Обов'язково використовуйте двофакторну аутентифікацію у всіх соціальних мережах, налаштуйте акаунти так, щоб особиста інформація була видна тільки друзям.
5. Не надсилайте фотографії своїх банківських карт, Google зберігає фото, тому краще їх видаляти.
6. Не використовуйте скрізь одні й ті ж паролі.

Поради для підвищення веб-безпеки і запобігання хакерським атакам [4]:

1. Створюйте надійні бекапи, виконуйте копіювання якомога частіше, розміщуйте їх в надійному та захищеному місці. Також допоможе відновити данні після хакерської атаки використання кількох бекапів.

2. Перейдіть з HTTP на HTTPS. Протокол HTTPS був розроблений якраз для шифрування та автентифікації в мережі. Додатковий рівень захисту створюють SSL та TLS, при роботі з платіжними операціями чи приватними даними користувачів це буде особливо необхідно.

3. Підтримуйте останню версію сайту, покращені функціональні можливості якраз забезпечують кращий рівень захисту.

4. Регулярно перевіряйте сайт на наявність багів та вразливих місць в безпеці і при виявлені негайно виправляйте.

5. Для того щоб швидко зреагувати коли сайт впав, виконуйте моніторинг аптайм і даунтайм сайту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безпека інформаційних систем [Електронний ресурс] // Режим доступу: https://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem

2. История нового взлома Sony [Електронний ресурс] // Режим доступу: https://habr.com/ru/post/364155/

3. Іранську АЕС атакував потужний комп'ютерний вірус [Електронний ресурс] // Режим доступу: https://tsn.ua/svit/iransku-aes-atakuvav-potuzhniy-komp-yuterniy-virus.html

4. Актуальні кіберзагрози 2017 і способи захисту від них [Електронний ресурс] // Режим доступу: https://internetdevels.ua/blog/cyber-threats-and-ways-to-prevent-them

Томчук Микола Антонович **—** доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: tomchuk@vntu.edu.ua

Риндін Сергій Анатолійович **—** студент групи 2ПІ-18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: rindin70@gmail.com

Tomchuk M. A. **—** Cand. Sc. (Eng.), Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: tomchuk@vntu.edu.ua

Sergii Ryndin **—** student of group 2PI-18m, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: rindin70@gmail.com