Атака Filecoder.Shade (січень 2019). Це вірус-шифрувальник, атака якого завжди починалась з отримання жертвою листа російською мовою з ZIP-архівом info.zip або inf.zip. У вкладенні, в середині архіву, знаходився завантажувач, який і загружав шифрувальника. Після зараження жертва отримувала інструкції з оплати російською та англійською мовами в TXT-файлі.

Наразі активно розповсюджується шкідливе програмне забезпечення, яке використовує WinRAR exploit (#CVE-2018-20250) (лютий- березень 2019). Дана прогармка надає можливість розпакувати файли з архіву в потрібну зловмисникам папку, а не призначену користувачем. Таким чином вони можуть помістити шкідливий код в папку автозавантаження Windows, який буде автоматично виконуватися при кожному завантаженні системи.

Сьогодні, під час підготовки до виборів, активно іде фішингова розсилка (28.03.2019) від імені Центру соціальних та маркетингових досліджень (SOCIS). Тому треба бути пильними.

Висновок. Для того щоб себе захистити від вірусів потрібно: мати антивірусні програми, правильно їх налаштувати; знати через які порти відбувається зараження і закрити їх; не переходити на підозрілі сторінки та не скачувати невідомі файли; під час встановлення програм не вимикати антивірусну програму; не водити свої дані на підозрілих сайтах. Значна частина атак відбувались через халатне ставлення людини до безпеки, отже потрібно проводити роз'яснювальну роботу серед користувачів щодо можливих шляхів зараження та навчати людей основним принципах захисту своїх комп'ютерів.

Список використаних джерел

1. Громадське [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://hromadske.ua/posts/naslidki-kiberataki
2. Cert [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://cert.gov.ua/news/56

УДК 004.056.5:004.75

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ ТЕХНОЛОГІЯХ

Полевод О.М., Трощилов М.О. студ гр. КБ-171
Базилевич В.М., доцент
Чернігівський Національний Технологічний Університет

Вступ. На сьогоднішній день хмарні сервіси стали настільки поширеними і тісно інтегрованими з обладнанням провідних виробників комп'ютерів і різних гаджетів, що багато хто навіть не замислюються про те, де саме зберігаються їхні дані і що з ними може статися. Хмарні обчислення — це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Основні поняття та визначення. Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем включають програмне забезпечення, тобто сервісну підсистему, та базу даних із багаторазовим доступом. Хмарний сервіс є особливою клієнт-серверною технологією, яка передбачає використання клієнтом ресурсів (процесорного часу, оперативної пам'яті, дискового простору, мережевих каналів, спеціалізованих контролерів, програмного забезпечення тощо) групи серверів у мережі, які взаємодіють наступним чином:

- для клієнта вся група виглядає як єдиний віртуальний сервер;
- клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб.

За допомогою провайдерів хмарних рішень можна орендувати через мережу Інтернет обчислювальні потужності та дисковий простір. Переваги такого підходу – доступність і можливість гнучкого масштабування. Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс. NIST США запропонував модель хмари, яка складається з п'яти основних характеристик, трьох моделей обслуговування і чотирьох моделей розгортання. Основні характеристики хмари:

- самообслуговування на вимогу;
- універсальний доступ по мережі;
- об'єднання ресурсів;
- облік споживання.
- Існують такі моделі обслуговування у хмарних технологіях:
- програмне забезпечення як послуга (SaaS); - користувач не купує SaaS-додаток, а
- орендує його
- платить за його використання деяку суму в місяць. SaaS провайдер піклується про

працездатність додатків, здійснює технічну підтримку користувачів, самостійно встановлює оновлення. Таким чином, користувач менше думає про технічну сторону питання, а зосереджується на своїх бізнес-цілях.

- платформа як послуга (PaaS) - модель надання хмарних обчислень, при якій споживач отримує

доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, зв'язного програмного забезпечення, засобів розробки і тестування розміщених у хмарних провайдерах.

– Інфраструктура як послуга (IaaS) - це модель обслуговування, в межах якої споживачу надається можливість керувати засобами обробки та збереження, комунікаційними мережами, та іншими фундаментальними обчислювальними ресурсами, на базі яких споживач може розгортати та виконувати довільне програмне забезпечення, до складу якого можуть входити операційні системи та прикладні програми.

Обчислювальна хмара може бути розгорнута як:

– хмара;
– громадська хмара;
– публічна хмара;
– гібридна хмара.

Проблемні питання захисту інформаціїї в хмарних технологіях. Головними проблемами, які потребують детального аналізу та вирішення, є такі:

– Проблема привілегійованих користувачів. Найбільшу загрозу для безпеки інформації в хмарі становлять користувачі, які мають привілейований доступ до функцій системи або адміністратори хмарних сервісів, тому для зменшення ризику можливих деструктивних дій з їх боку, доцільно вести незалежний нагляд та контроль за їх діями в хмарі.

– Однією з головних проблем, що гальмує поширення хмарних обчислень, є невідповідність законів у сфері обробки, передачі, збереження та захисту інформації різних держав. Вирішення цієї проблеми є ключовим фактором для можливості фізичного розміщення серверів постачальника хмарних сервісів у різних країнах та регіонах.

– Питання довіри до постачальника послуг можуть бути вирішені лише за рахунок проведення аудиту безпеки постачальника хмарних послуг та перевірки відповідності його системи безпеки міжнародним вимогам до захисту інформації, що сформульовані в міжнародних стандартах.

– Питання загальних вразливостей у хмарі практично нічим не відрізняються від аналогічних у традиційних системах, за винятком того, що знайдена одна вразливість може бути використана для всієї хмари.І в цей час її критичність набагато більша, бо вона може з легкістю уразити всіх користувачів даного постачальника послуг.

– Проблеми доступності до сервісів та даних користувачами, відновлення їх роботи після збоїв, чи втрати даних повинні вирішуватися на адміністративному та правовому рівнях. При укладанні договорів з користувачем мають бути чітко визначені обов'язки сторін та міра їх відповідальності в залежності від обставин події, що призвела до цих наслідків, а розслідування повинна проводити третя незалежна сторона.

– Проблема надання доступу, спільного доступу та блокування доступу до ресурсів і даних у хмарі користувачам та проблема захисту інтелектуальної власності в хмарі, зокрема програмного забезпечення та даних.

Висновки. Отже, із проведеного нами дослідження можна зробити наступні висновки: Питання інформаційної безпеки технології хмарних сервісів потребують значного вдосконалення, а в багатьох аспектах – першочергових розробок і напрацювань. Зі всією сукупністю переваг, які надає використання хмарних обчислень, є багато питань безпеки, які на сьогодні не достатньо добре проаналізовані та знаходяться ще на стадії обговорення.

Список використаних джерел

1. Щурська М. О. аналіз питань інформаційної безпеки в хмарних сервісах [Електронний ресурс] / М. О. Щурська, Т. В. Литвинова – Режим доступу до ресурсу: http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2015/05/Shchurska-Publication.pdf.

2. Основні поняття хмарних технологій [Електронний ресурс] – Режим доступу до ресурсу: http://academicfox.com/lektsiya-1-osnovni-ponyattya-hmarnyh-tehnolohij/.

3. Хмарні технології. Переваги і недоліки. [Електронний ресурс] – Режим доступу до ресурсу: https://valtek.com.ua/ua/system-integration/it-infrastructure/clouds/cloud-technologies