УДК 62.503.55

Єніна І.І., Рибак І.Ю.
Центральноукраїнський національний технічний університет

Кібербезпека в хмарному середовищі. Watering Holes та Фішинг

За словами Стефано Ортолані, хоча рівень захищеності «хмар» чимало залежить від самих провайдерів, користувачам все-таки варто гарненько подумати, які з файлів довіряти «хмаросховищам».

Хмарне сховище даних – модель онлайн сховища, в якому дані зберігаються на багаточисельних серверах в мережі, які надаються для користуванням клієнтам третьою стороною.[1]

До моделей використання відносяться традиційні: IaaS (оренда IT-інфраструктури), SaaS (оренда додатків), PaaS (розробка додатків).

Нещодавно з'явились BPaaS (послуги по рішенню бізнес-задач), DaaS (віртуальна робоча стільниця), SecaaS (інформаційна безпека в оренду), BaaS (резервне копіювання, як сервіс), DRaaS (рішення по забезпеченню катастрофостійкості), CCaaS (віртуальний контакт-центр).[2]

В даний час користувачу дозволяють обрати між різними сервісами зберігання даних. Найбільш поширеними є наступні сервіси:

- Google Drive – до сервісу можна отримати доступ як з сайту, так і із спеціально створених для цього додатків в Windows, Mac OS, Android, IOS.

За умовами, користувачу надається безкоштовно 15Гб пам'яті[3] для зберігання своїх даних, також, можливі деякі безкоштовні акції, за умовами яких можуть надавати додатковий простір. Так, в 2016 році за перевірку безпеки, надавали 2Гб додаткового простору безкоштовно. Якщо необхідна велика кількість додаткового простору, то його можна купити за деяку суму. В даний час, на листопад 2016 року, доступно 15Гб безкоштовно, 100Гб, 1Тб, 30, 20, 30Тб - за кошти (наприклад, 30Тб за 6 899грн/міс).

- Dropbox – в лютому 2014 перейменований на Microsoft SkyDrive, базується на інтернет-сервісі зберігання даних з функціями файлообміну. Безкоштовно дається 5Гб, а по різним акціям можна отримати додатковий дисковий простір.

- Хмара@mail.ru – дається безкоштовно 25Гб пам'яті.

Існують і інші сервіси, серед них Mega, Яндекс.Диск, OAmazon Web Services, ADrive, Bitcasa, Yunpan 360, 4shared, SugarSync, Box.net, iDrive, OpenDrive, Syncplicity, MediaFire, Cubby.com.[4]

Якщо проаналізувати статистику втрат даних з хмарних сховищ, то можна виділити короткий перелік порад, які допоможуть підвищити безпеку даних.

Одна з причин, яка спричиняє заволодіння доступом до даних зловмисниками є нехтування правил безпеки по підбору пароля. Дуже часто, щоб не забивати голову різними паролями, люди використовують один пароль для найрізноманітніших сайтів. Зазвичай, це номер телефона, електронна пошта або логін (в залежності від сервісу). Далі, зловмисник зламавши профіль на сайті з низьким рівнем безпеки, зможе без перешкод зайти на інший сервіс простою підстановкою того ж пароля. Чим складніше буде пароль, тим важче його зламати. Найкраще використовувати паролі з використанням літер різного регістру, цифр та символів.

Для того, щоб точно зберегти свої дані, зберігати їх потрібно на різних хмарних сервісах, використовувати різні паролі для доступу до них. Такі сервіси, як Otixo або Primadesk дозволять отримати доступ до всієї інформації з одного місця. Задавати непублічний тип інтернет-з'єднання, а також перевіряти посилання за якими відбувається перехід та шифрувати дані. Але всі ці поради лише зменшать ризик і ніяк не зможуть повністю попередити їх втрату. [5] Якщо брати до уваги саме хакерські атаки, то найбільш поширеними видами атак є направлений фішинг та "Watering Holes". При фішингу, зловмисники можуть написати електронного листа легітимному працівнику від імені його колеги по роботі, де запитати персональні дані і отримати відповідь із правдивими даними. Дуже велика кількість користувачів

інтернет-сервісів не мають мінімальних знань по безпеці в мережі, а саме, що сервіси не розсилають листів з проханнями повідомити у відповідь особисті дані (паролі, логіни, номера телефонів тощо).

В травні 2008 року в соціальній мережі ВКонтакті масово поширився даний тип атаки і за оцінками спеціалістів, більш ніж 70% атак – успішні.[6]

Статичні захисні механізми, до яких відносяться системи розмежування доступу, системи аутентифікації, в багатьох випадках не можуть забезпечити ефективного захисту. Тому потрібні динамічні методи, що дозволять оперативно виявляти та запобігати порушення безпеки.[7]

Для боротьби проти фішингу розроблено багато методів: браузери, які попереджають про загрозу фішинга, посилена процедура авторизації, спам-фільтри, послуги моніторингу, юридичні міри.

При Watering Holes хакери розміщюють програми в коді сайту. В результаті таких дій, користувач, переходячи на сайт, може передати вірус у всю мережу підприємства, а хакер отримає доступ до даних цієї мережі.

В 2014 році компанія Dell зібрала близько 37 мільйонів унікальних зразків, що майже в два рази більше ніж в 2013 році. Найбільше від цих атак страждають представники малого та середнього бізнесу, тому що не виділяють необхідні кошти на безпеку і як результат несуть величезні збитки. За статистикою[10], близько 60% підприємств в Об'єднаному королівстві припиняють свою роботу після злому. Зазвичай причиною є відсутність бізнес-плану на випадок такої атаки. Найбільш часто, малі та середні підприємства, використовують наступні способи захисту даних від розповсюджених атак: неперервне шифрування - в результаті часу витрачається небагато, а швидкість передачі залишається швидкою; розширена аутендифікація - носить в собі комбінацію аутендифікацій; стримання загроз - програми стримання загроз автоматично [11].

Розпізнають та зупиняють загрози ще до того, як вони змогли потрапити на комп'ютер або в мережу. До того ж, програма базується на поведінкових факторах, тому вона може попередити розповсюдження атак zero-day.

В 2010 році Аза Раскин представив метод боротьби з фішингом Tabnabbing. Його мета полягала в наступному: атакуючий заманює користувача на сторінку свого сайту, яка виглядає абсолютно нормальною і такою, якою користувач очікує її побачити. Вираховує, що користувач тривалий час не взаємодіяв з сторінкою, або взагалі перемкнувся на іншу вкладку. Поки сторінка неактивна – підмінюється її favicon на іконку сайта, під якою вона буде маскуватись. Контент сторінки змінюється на контент фейкової форми логіна веб-сайту, під якою вона маскується. З достатньо великою ймовірністю, користувач, повернувшись до вкладки – не задумуючись, автоматично введе свій логін та пароль. Після перехоплення даних авторизації – користувача можна переадресувати на атакуємий сайт, адже, найчастіше, він на ньому вже авторизований і саме цієї поведінки він і буде очікувати.[12]

В даний час дуже важливе питання безпечного зберігання даних в хмарах, тому розробка методів захисту є надзвичайно актуальною.

Список використаних джерел

1. *Облачное_хранилище_данных – загальні дані про хмарні сервіси [Електронний ресурс]. – Режим доступу:* https://ru.wikipedia.org/wiki/
2. *Что такое облака? Мифы о них в головах IT-шников: мнения, стереотипы и жизнь в облаках [Електронний ресурс]. – Режим доступу:* https://habrahabr.ru/company/simnetworks/blog/308266/
3. Gmail + GDrive = теперь 15 гигабайт бесплатно *[Електронний ресурс]. – Режим доступу:* https://geektimes.ru/post/179569/
4. *Огляд 10ти хмарних сховищ даних [Електронний ресурс]. – Режим доступу:* http://www.topobzor.com/obzor-10-oblachnyx-xranilishh-dannyx/.html
5. *Как защитить данные в облаке от кражи [Електронний ресурс]. – Режим доступу:* http://www.lookatme.ru/mag/how-to/security/208511-cloud-security
6. *Пользователи сайта "ВКонтакте.ру" стали жертвами компьютерного вируса [Електронний ресурс]. – Режим доступу:* https://ria.ru/society/20080516/107610576.html
7. *Єніна І. Методи захисту комп'ютерних мереж від хакерських атак / І.Єніна, А.Ковтунов // Збір. наук. праць КНТУ/ Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Кіровоград. КНТУ, – 2011. –Вип. 24.*
8. *AOL phishing fraudster found quilty [Електронний ресурс]//Вікіпедія. – Режим доступу:* http://www.theregister.co.uk/2007/01/17/aol_phishing_fraudster/
9. *Man Found Guilty of Targeting AOL Customers of Phishing Scam [Електронний ресурс]. – Режим доступу* http://www.pcmag.com/article2/0,2817,2085182,00.asp
10. *Статистика підприємств, які зазнали краху через зломи [Електронний ресурс]. – Режим доступу:* https://aerissecure.com/blog/smb-data-breach-fallout/
11. *Последствия кибератак для малого и среднего бизнеса [Електронний ресурс]. – Режим доступу:* http://hi-tech.ua/blog/posledstviya-kiberatak-dlya-malogo-i-srednego-biznesa/
12. *Tabnabbing: экстравагантный фишинг [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/236387/.*