УДК 004.75

Струбицький П. Р., Струбицький Р. П., Шаховська Н. Б.

АНАЛІЗ ЗАГРОЗ ХМАРКОВИМ СХОВИЩАМ ДАНИХ ТА МЕТОДІВ ЇХ ЗАХИСТУ

Проведено аналіз загроз безпеки в хмаркових сховищах даних. Класифіковано на основі віртуалізації виявлені потенційні загрози. Враховано особливості кожного типу загроз. Розроблено методи і засоби захисту залежно від класу потенційних загроз.

Ключові слова: *хмаркові обчислення, сховища даних, захист.*

Проведен анализ угроз безопасности в облачных хранилищах данных. Классифицированы на основе виртуализации выявленные потенциальные угрозы. Учтены особенности каждого типа угроз. Разработаны методы и средства защиты в зависимости от класса потенциальных угроз.

Ключевые слова: *облачные вычисления, хранилища данных, защита.*

The paper analyzed the security threats cloud data storage. Classification of identified threats and potentiality based virtualization. Given the characteristics of each type of threat. The methods of protection, depending on the class of potential threats.

Key words: *clouds computing, data storage, protection.*

Постановка проблеми. Хмаркові сховища даних представляють собою сукупність серверів, які розміщені на одній чи декількох площадках з метою підвищення ефективності та захищеності. Захист хмаркових сховищ даних представляє собою мережевий та фізичний захист, а також відмовостійкість і надійне електропостачання.

Нині на ринку представлено широкии спектр рішень для захисту серверів і сховищ від різноманітних загроз. Їх об'єднує орієнтованість на вузький спектр вирішуваних задач. Проте спектр цих задач дещо розширився внаслідок поступового витіснення класичних апаратних систем віртуальними платформами.

До відомих типів загроз (мережеві атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) добавились складнощі, що пов'язані з контролем середовища, трафіком між гостьовими машинами та розмежуванням прав доступу. Розширилися внутрішні питання і політики захисту хмаркових сховищ даних, вимоги зовнішніх регуляторів.

У сучасних умовах стає все складніше забезпечити захист критично важливих для бізнесу систем і додатків.

Аналіз останніх досліджень та публікацій. Робота сучасних сховищ даних у низці галузей вимагає закриття технічних питань, а також питань, пов'язаних із їх безпекою. Фінансові інститути (банки, процесингові центри) підпорядковані багатьом стандартам, виконання яких закладено на рівні технічних рішень. Проникнення платформ віртуалізації досягло того рівня, коли практично всі компанії, що використовують ці системи, вельми серйозно зайнялися питаннями посилення безпеки в них. Зазначимо, що буквально рік тому інтерес був скоріше теоретичний [1; 3; 5].

Постановка завдання. Поява віртуалізації стала актуальною причиною масштабної міграції більшості систем на віртуальні машини, проте рішення задач забезпечення безпеки, пов'язаних з експлуатацією додатків у новому середовищі, вимагає особливого підходу. Багато типів загроз достатньо вивчені, і для них розроблено засоби захисту, проте їх ще потрібно адаптувати для використання в хмарі.

Для достатньо ефективного впровадження хмаркових сховищ даних в усі галузі потрібно детально проаналізувати види та типи загроз безпеці хмаркових сховищ даних і на основі цього виробити механізми протидії.

Виклад основного матеріалу дослідження. Розгляд безпеки хмарних сховищ даних доцільно почати з аналізу існуючих загроз. Враховуючи те, що хмарні сховища є частиною технології хмаркових обчислень, можна вважати, що всі існуючі загрози для останніх також є потенційними загрозами для хмаркових сховищ.

Контроль і управління хмарками є проблемою безпеки, оскільки немає гарантій, що всі ресурси хмарки підраховані і в ній немає неконтрольованих віртуальних машин, незапущених зайвих процесів і не порушена взаємна конфігурація елементів хмарки. Це високорівневий тип загроз, тому що він пов'язаний з керованістю хмаркою, як єдиною інформаційною системою і для неї загальний

захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмаркових інфраструктур [7].

В основі забезпечення фізичної безпеки лежить суворий контроль фізичного доступу до серверів і мережевої інфраструктури. На відміну від фізичної безпеки, мережева безпека в першу чергу представляє собою побудову надійної моделі загроз, що включає в себе захист від вторгнень і міжмережевий екран. Використання брандмауера передбачає роботу фільтра, з метою розмежувати внутрішні мережі хмарки на підмережі з різним рівнем довіри. Це можуть бути окремі сервери, які доступні з Інтернету або сервери з внутрішніх мереж.

У хмаркових обчисленнях найважливішу роль платформи виконує технологія віртуалізації. Для збереження цілісності даних і забезпечення захисту розглянемо основні відомі загрози для хмаркових обчислень, які базуються на віртуалізації [5]. Їх можна згрупувати за категоріями:

1. Труднощі при переміщенні звичайних серверів у хмари.
2. Динамічність віртуальних машин.
3. Уразливості всередині віртуального середовища.
4. Захист бездіяльних віртуальних машин.
5. Захист периметра і розмежування мережі.

Труднощі при переміщенні звичайних серверів в хмари викликані декількома чинниками. Вимоги до безпеки хмаркових обчислень не відрізняються від вимог безпеки до центрів обробки даних чи інших комп'ютерних систем аналогічного призначення. Однак віртуалізація і перехід до хмаркових середовищ призводять до появи нових загроз.

Доступ через Інтернет до управління обчислювальною потужністю – одна з ключових характеристик хмарних обчислень. У більшості традиційних сховищ доступ інженерів до серверів контролюється на фізичному рівні, в хмаркових середовищах вони працюють через Інтернет. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одним з головних критеріїв захисту.

Динамічність віртуальних машин також створює потенційність загроз. Створити нову машину, зупинити її роботу, запустити заново можна за короткий час. Вони клонуються і можуть бути переміщені між фізичними серверами. Ця мінливість важко впливає на розробку цілісності системи безпеки. Однак уразливості операційної системи або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються після довільного проміжку часу. У середовищах хмаркових обчислень важливо надійно зафіксувати стан захисту системи, при цьому це не повинно залежати від її стану та місця розташування.

Уразливості всередині віртуального середовища охоплює загрози під час функціонування. Сервери хмаркових обчислень і локальні сервери використовують одні й ті ж операційні системи та програми. Для хмарних систем загроза віддаленого злому або зараження шкідливим програмним забезпеченням висока. Ризик для віртуальних систем також високий. Паралельні віртуальні машини збільшують «атакований простір». Система виявлення та запобігання вторгнень має бути здатною виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарковому середовищі.

Захист бездіяльних віртуальних машин впливає на безпеку. Коли віртуальна машина вимкнена, вона наражається на небезпеку зараження. Доступу до сховища образів віртуальних машин через мережу достатньо. На виключеній віртуальній машині абсолютно неможливо запустити захисне програмне забезпечення. У цьому випадку повинен бути реалізований захист не тільки всередині кожної віртуальної машини, а й на рівні гіпервізора.

Захист периметра і розмежування мережі при хмарному зберіганні даних виділяється в окрему загрозу. При використанні хмарних обчислень периметр мережі розмитий або зникає. Це призводить до того, що захист менш захищеної частини мережі визначає загальний рівень захищеності. Для розмежування сегментів з різними рівнями довіри в хмарі віртуальні машини повинні самі забезпечувати себе захистом, переміщаючи мережевий периметр до самої віртуальної машини. Корпоративний брандмауер – основний компонент для впровадження політики IT-безпеки та розмежування сегментів мережі, не в змозі вплинути на сервери, розміщені в хмарних середовищах.

Потенційні атаки на хмари і на хмарні сховища доцільно розглядати в сукупності з рішеннями для їх усунення.

1. Традиційні атаки на програмне забезпечення.

Уразливості операційних систем, модульних компонентів, мережевих протоколів – традиційні загрози, для захисту від яких досить встановити міжмережевий екран, антивірус, IPS та інші компоненти. При цьому важливо, щоб ці засоби захисту ефективно працювали в умовах віртуалізації.

2. Функціональні атаки на елементи хмари.

Цей тип атак пов'язаний з шаруватістю хмари, загальним принципом безпеки. Для захисту від функціональних атак для кожної частини хмари необхідно використовувати такі засоби захисту: для проксі – ефективний захист від DoS-атак, для веб-сервера – контроль цілісності сторінок, для сервера додатків – екран рівня додатків, для СУБД – захист від SQL-ін'єкцій, для системи зберігання даних – правильне резервне копіювання, розмежування доступу. Окремо кожні з цих захисних механізмів вже створені, але вони не зібрані разом для комплексного захисту хмари, тому завдання щодо інтеграції їх в єдину систему потрібно вирішувати під час створення хмари.

3. Атаки на клієнта.

Більшість користувачів підключаються до хмари, використовуючи браузер. Тому можна розглядати такі атаки, як Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій.

Єдиний захист від цього виду атак є правильна аутентифікація та використання шифрованого з'єднання з взаємною аутентифікацією. Однак ці методи захисту не дуже зручні і дуже марнотратні для творців хмар. У цій галузі інформаційної безпеки є ще багато невирішених завдань.

4. Атаки на гіпервізор.

Гіпервізор є одним з ключових елементів віртуальної системи. Основною його функцією є поділ ресурсів між віртуальними машинами. Атака на гіпервізор може призвести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину з сервера. У ролі стандартних методів захисту рекомендується застосовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів зі службою каталогів Active Directory, використання політик складності і старіння паролів, а також стандартизацію процедур доступу до управляючих засобів хост-сервера, застосовувати вбудований брандмауер хоста віртуалізації. Також можливе відключення таких часто невикористовуваних служб як, наприклад, веб-доступ до сервера віртуалізації.

5. Атаки на системи управління.

Велика кількість віртуальних машин, що використовуються в хмарах вимагає наявність систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може призвести до появи віртуальних машин-невидимок, здатних блокувати одні віртуальні машини і підставляти інші.

Найбільш ефективні способи захисту в галузі безпеки хмар опублікувала організація Cloud Security Alliance (CSA) [6]. Проаналізувавши опубліковану підприємством інформацію, було запропоновано такі рішення.

1. Збереження даних, шифрування.

Шифрування – один із найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію клієнта, що зберігається в хмарці, а також, у випадку відсутності необхідності, безповоротно видаляти.

2. Захист даних при передачі.

Зашифровані дані при передачі повинні бути доступні тільки після аутентифікації. Дані не вийде прочитати або зробити в них зміни, навіть у випадку доступу через ненадійні вузли. Такі технології досить відомі, оскільки алгоритми та надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

3. Аутентифікації – захист паролем.

Для забезпечення більш високої надійності часто вдаються до таких засобів, як токени та сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації, також рекомендується використовувати LDAP (полегшений протокол доступу до каталогів) і SAML (Security Assertion Markup Language).

4. Ізоляція користувачів.

Використання індивідуальної віртуальної машини і віртуальної мережі. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service). Часто провайдери ізолюють дані користувачів один від одного за рахунок зміни даних коду в єдиному програмному середовищі. Цей підхід має ризики, пов'язані з небезпекою знайти дірку в нестандартному коді, що дозволяє отримати доступ до даних. У випадку можливої помилки в коді користувач може отримати дані іншого. Останнім часом такі інциденти часто мали місце.

Висновки дослідження і перспективи подальших розвідок у цьому напрямі. Описані рішення із захисту від загроз безпеки хмарних обчислень застосовуються системними інтеграторами в проектах побудови приватних хмар. Після застосування цих рішень кількість інцидентів істотно знижується. Але багато проблем, пов'язаних із захистом віртуалізації, вимагають ретельного аналізу і опрацьованого рішення.

ЛІТЕРАТУРА

1. Cloud Security Alliance [Електронний ресурс]. – Режим доступу : https://cloudsecurityalliance.org/.
2. Cloud Standards Summit. OMG Standards in Government & NGO's Workshop [Електронний ресурс]. – Режим доступу : http://www.omg.org/news/meetings/GOV-WS/css/index.htm.
3. GDV Data Protection Blog [Електронний ресурс]. – Режим доступу : http://www.globaldatavault.com/blog/for- magnolia-not-so-well-done/.
4. IBM Security NetworkIntrusion Prevention System [Електронний ресурс]. – Режим доступу : http://public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/ WGD03002USEN.PDF.
5. Open Data Center Alliance [Електронний ресурс]. – Режим доступу : http://www.opendatacenteralliance.org/.
6. Organization for the Advancement of Structured Information Standards [Електронний ресурс]. – Режим доступу : http://www.oasis-open.org/org/.
7. Press Release. Major Standards Development Organizations Collaborate to Further Adoption of Cloud Standards [Електронний ресурс]. – Режим доступу : http://cloud-standards.org/wiki/ index.php?title=Press_Release.
8. Virtual desktop malware defence [Електронний ресурс]. – Режим доступу : http://www.dennistechnologylabs.com/ reports/security/anti-malware/symantec/DTL_SYM_VDI.pdf.
9. Облачные сервисы на платформе HP CloudSystem [Електронний ресурс]. – Режим доступу : http://storagenews.ru/46/HP_CloudService_46.pdf.

Дата надходження статті до редколегії 07.10.2013 р.

СТРУБИЦЬКИЙ Павло Романович – кандидат технічних наук, доцент кафедри економічної кібернетики та інформатики Тернопільського національного університету, м. Тернопіль.
Коло наукових інтересів: інтелектуальний аналіз даних, сховища даних.

СТРУБИЦЬКИЙ Ростислав Павлович – аспірант Національного університету «Львівська політехніка», м. Львів.
Коло наукових інтересів: сховища даних, хмаркові технології, платіжні системи.

ШАХОВСЬКА Наталія Богданівна – доктор технічних наук, доцент, професор кафедри інформаційних систем та мереж Національного університету «Львівська політехніка», декан базової освіти інституту комп'ютерних наук та інформаційних технологій Національного університету «Львівська політехніка», м. Львів.
Коло наукових інтересів: сховища та простори даних.