УДК 004.492.2

Ігор Володимирович КОБЗЕВ,
кандидат технічних наук, доцент,
доцент кафедри природознавчих наук
Харківського національного університету радіоелектроніки;
Катерина Костянтинівна ПЕТРОВА,
студентка Харківського національного університету радіоелектроніки

ХМАРНІ ОБЧИСЛЕННЯ ТА КІБЕРБЕЗПЕКА ЕЛЕКТРОННОГО УРЯДУ

Глобальний тренд розвитку інформатизації державних структур полягає в переведенні значної частини інформаційної інфраструктури у хмарні технології. Це дозволяє зменшити значну частину капітальних вкладень переорієнтував їх в операційні витрати, скоротити затрати і прискорити цикл запровадження нових рішень.

Стимулом до поширення хмарних технологій в держсекторі являються такі чинники, як стратегія держави в галузі електронного врядування, законодавчі ініціативи в галузі персональних даних, зростання вимог до оперативності роботи держустанов і збільшення кількості державних послуг, до яких громадяни мають доступ у електронному вигляді.

У тому, що хмарні технології необхідні для створення ефективної держави, сьогодні ніхто не має сумніву. Проте чиновники часто не квапляться їх впроваджувати. По-перше, державні установи не знають які сервіси і дані перемістити в хмару, а які залишити у себе на локальних серверах. По-друге, при переході до хмар, у керівництва виникають природні сумніви в їх надійності і безпеці та відповідності таких технологій діючому законодавству. По-третє, існує відома бюрократична звичка якщо не утаємничувати, то, принаймні, не ділитися «власними» даними з іншими користувачами [1].

Ще в 2016 році до Верховної Ради України було внесено законопроект про хмарні технології № 4302 [2], над яким працює комітет ВРУ з інформаційних технологій разом з Американською Торгівельною Палатою в Україні.

Хоча бізнес уже давно використовує переваги хмарних рішень у своїй роботі, створення правової бази для переходу держсектору на «хмару» є необхідним для повноцінного розвитку системи е-врядування.

Спільна робота над законопроектом свідчить про готовність державного, приватного та громадського секторів працювати разом над впровадженням в Україні е-врядування.

Використання електронних систем є одним зі засобів дебюрократизації процесу управління освітою, що має бути відкритим та основаним на фактах [3].

Центр обробки даних (ЦОД) є сукупністю серверів, розміщених на одному майданчику з метою підвищення ефективності і захищеності. Захист центрів обробки даних здійснюється мережним і фізичним засобами. Нині на ринку представлений широкий спектр рішень для захисту серверів і ЦОД від різних загроз. Їх об'єднує орієнтованість на вузький спектр вирішуваних завдань. Проте спектр цих завдань піддався деякому розширенню внаслідок поступового витіснення класичних апаратних систем віртуальними платформами. До відомих типів загроз (мережні атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) додалися складнощі, пов'язані з контролем середовища, трафіку між гостьовими машинами і розмежуванням прав доступу. Розширилися внутрішні питання і політики захисту ЦОД, вимоги зовнішніх регуляторів. Робота сучасних ЦОД у низці галузей вимагає вирішення технічних питань, а також питань пов'язаних з їх безпекою. Державні інститути повинні дотримуватися низки стандартів, виконання яких закладене на рівні технічних рішень. Проникнення платформ віртуалізації досягло того рівня, коли практично усі компанії, які використовують ці системи, дуже серйозно зайнялися питаннями посилення безпеки в них. У сучасних умовах стає все складніше забезпечити захист критично важливих для бізнесу систем і додатків.

Поява віртуалізації стала актуальною причиною масштабної міграції більшості систем в «хмару», проте вирішення завдань забезпечення безпеки, пов'язаних з експлуатацією застосувань в новому середовищі, вимагає особливого підходу. Багато типів загроз вивчено і для них розроблені засоби захисту, проте їх ще треба адаптувати для використання в хмарі.

Контроль і управління хмарами — є проблемою безпеки. Гарантій, що усі ресурси хмари прораховані і в ній немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари немає. Це високорівневий тип загроз, оскільки він пов'язаний з керованістю хмарою як єдиною інформаційною системою і для нього загальний захист треба будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

У основі забезпечення фізичної безпеки лежить регулярний контроль фізичного доступу до серверів і мережевої інфраструктури. На відміну від фізичної безпеки, мережева безпека в першу чергу базується на побудові надійної моделі загроз, що включає захист від вторгнень і міжмережний екран. Використання міжмережного екрану має на увазі роботу фільтру, з метою розмежувати внутрішні мережі ЦОД на підмережі з різним рівнем довіри. Це можуть бути окремі сервери, що доступні з Інтернету або сервери з внутрішніх мереж.

У хмарних обчисленнях найважливішу роль платформи виконує технологія віртуалізації. Для збереження цілісності даних і

забезпечення захисту розглянемо основні відомі загрози для хмарних обчислень.

Труднощі при переміщенні звичайних серверів в обчислювальну хмару. Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Проте, віртуалізація ЦОД і перехід до хмарних середовищ призводять до появи нових загроз.

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

Віртуальні машини динамічні. Створити нову машину, зупинити її роботу, запустити наново можна за короткий час. Вони клонуються і можуть бути переміщені між фізичними серверами. Ця мінливість суттєво впливає на розробку цілісності системи безпеки. Проте, уразливості операційної системи або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються після довільного проміжку часу (наприклад, при відновленні з резервної копії). У середовищах хмарних обчислень важливо надійно зафіксувати стан захисту системи, при цьому це не повинно залежати від її стану і місця розташування.

Наступним видом загроз є уразливості всередині віртуального середовища. Сервери хмарних обчислень і локальні сервери використовують одні і ті ж операційні системи та додатки. Для хмарних систем загроза видаленого зламу або зараження шкідливим ПЗ є достатньо високою. Ризик для віртуальних систем також є високим. Паралельні віртуальні машини збільшує «поверхню», що атакується. Система виявлення і запобігання вторгненням має бути здатна виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарному середовищі.

Коли віртуальна машина вимкнена, вона наражається на небезпеку зараження. Доступу до сховища образів віртуальних машин через мережу вистачає. На вимкненій віртуальній машині абсолютно неможливо запустити захисне програмне забезпечення. У даному випадки є можливість реалізувати захист не лише усередині кожної віртуальної машини, але і на рівні гіпервізора.

Захист периметру і розмежування мережі також є важливою складовою процедури захисту хмар. При використанні хмарних обчислень периметр мережі «розмивається» 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.

Розглянемо деякі види атак на хмарні сервіси.

1. Традиційні атаки на ПЗ. Уразливості операційних систем, модульних компонентів, мережевих протоколів і ін.

2. Функціональні атаки на елементи хмари. Цей тип атак пов'язаний з багатошаровістю хмари, загальним принципом безпеки.

3. Атаки на клієнта. Більшість користувачів підключаються до хмари, використовуючи браузер. Такими видами атак є Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій, «людина посередині» і багато інших.

4. Атаки на гіпервізор. Гіпервізор є одним з ключових елементів віртуальної системи. Основною його функцією є розподіл ресурсів між віртуальними машинами. Атака на гіпервізор може привести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів інший. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину з сервера.

5. Атаки на системи управління. Велика кількість віртуальних машин, що використовується в хмарах вимагає наявності систем управління, здатних надійно контролювати створення, перенесення і утилізацію віртуальних машин.

В [4] наведено найбільш ефективні способи захисту в галузі безпеки хмар. Розглянемо їх.

1. Шифрування – один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у випадки відсутності необхідності, безповоротно видаляти. Зашифровані дані при передачі мають бути доступні тільки після аутентифікації. Дані не вийде прочитати або зробити зміни, навіть у випадки доступу через ненадійні вузли. Такі технології досить відомі, алгоритми і надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

2. Автентифікація – захист паролем. Для забезпечення більш високої надійності, часто використовують такі засоби, як токени і сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації, також рекомендується використовувати LDAP (Lightweight Directory Access Protocol) і SAML (Security Assertion Markup Language).

3. Використання індивідуальної віртуальної машини і віртуальної мережі. Віртуальні мережі мають бути розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service).

Можна стверджувати, що хмарні технології є однією з основних технологічних баз для сучасної ефективної організації електронної інформаційної взаємодії державних органів, зокрема побудови системи електронного урядування.

Висновок. Кібербезпека електронного уряду при розміщенні інформації в хмарах на теперішній час є дуже актуальним питанням.

Описані вище рішення щодо захисту від загроз безпеки хмарних обчислень неодноразово були застосовані системними інтеграторами в проектах побудови приватних хмар. Після застосування цих рішень кількість інцидентів, що сталися, істотно знизилася. Але багато проблем, пов'язаних із захистом хмар ще вимагають ретельного аналізу і вирішення.

Список бібліографічних посилань

1. Kobzev I. V., Melnikov O. F., Orlov O. V. Cloud technology and e-government // Current scientific research: Collection of scientific articles. Publishing house «BREEZE», Montreal, Canada, 2017. P. 159-163.

2. Проект Закону про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень : законопроект № 4302 від 24.03.2016 // БД «Законопроекти» / Верховна Ради України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511= 58527 (дата звернення: 09.10.2018)

3. Греба Р. Електронне врядування-2017: досягнення і перспективи // Українська правда. 09 січня 2018 09:30. URL: https://www.pravda.com.ua/ columns/2018/01/9/7167821/ (дата звернення: 09.10.2018).

4. Threats of cloud computings and methods was more their than protection // Developers Club geek daily blog. June 2013. URL: http://developers-club.com/ posts/183168/ (дата звернення: 09.10.2018).

Одержано 10.10.2018

УДК 004.658

Олександр Олександрович КОВАЛЬОВ,
аспірант 2 курсу
Ужгородського національного університету

ЗАХИСТ ВІД СЛІПИХ SQL-ІН'ЄКЦІЙ ЗА ДОПОМОГОЮ ПРАВИЛЬНОЇ ОБРОБКИ ПОМИЛОК НА СТОРОНІ АРІ

SQL-ін'єкція – один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

Впровадження SQL, залежно від типу СКБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері.

Основна небезпека до якої може вести вдало проведена атака SQL-ін'єкцією – це повна втрата інформації з БД. Добре якщо там немає нічого цінного, але, в залежності від обставин, частіше за все в БД зберігається багато досить критичних даних: облікові записи користувачів (включаючи паролі), номери телефонів, адреси