а) оцінювати масштаби використання трудових ресурсів, потенціалу створення робочих місць за окремими групами та категоріями зайнятих, особливості укладання трудових угод з різними категоріями персоналу, специфіку зайнятості в малому підприємництві;

б) аналізувати політику та форми оплати праці в малому бізнесі;

в) розглядати проблеми організації, умов і охорони праці на малих підприємствах, у тому числі меж робочого часу;

г) оцінювати прийнятні для підприємців умови використання в малому бізнесі праці соціально вразливих на ринку праці категорій населення;

д) оцінювати роль інституціонального середовища в забезпеченні соціальної захищеності працівників;

є) аналізувати установки обласної програми розвитку малого підприємництва в аспекті стимулювання залучення в малий бізнес трудових ресурсів;

ж) аналізувати практичну потребу на сьогодні нормативно-правової бази використання трудових ресурсів у малому підприємництві.

Список літератури

1. Офіційний сайт Кіровоградського обласного центру зайнятості / [Електронний ресурс]. – Режим доступу: www.dcz.gov.ua.

2. Офіційний сайт Головного управління статистики в Кіровоградській області / [Електронний ресурс]. – Режим доступу: www.kr.ukrstat.gov.ua.

УДК 004.056

КЛАСИФІКАЦІЯ ЗАГРОЗ ВІРТУАЛЬНОЇ ХМАРНОЇ ІНФРАКСТРУКТУРИ

Ладигіна О.А., асист.
Кіровоградський національний технічний університет

В даний час одночасно з бурхливим розвитком концепції хмарних обчислень, коли обчислювальна інформаційна послуга як сервіс повністю відокремлена від рівня зберігання і надання доступу до цієї послуги, знаходять своє застосування віртуальні середовища в якості основи для розгортання хмарної інфраструктури. З урахуванням широкого застосування систем віртуалізації від рівня інформаційної захищеності віртуального середовища та інфраструктури безпосередньо залежить захищеність усієї хмарної інфраструктури [1-2].

При класифікації загроз інформаційної безпеки з принципових способів їх реалізації стосовно до архітектури всієї віртуальної хмарної інфраструктури в сукупності виділяються три групи загроз:

- для платформи віртуального середовища;
- викликані проблемами конфігурації віртуального середовища;
- стандартні загрози реального середовища в віртуальному просторі.

Також є свої види загрози для кожної з основних моделей надання хмарних сервісів:

1. IaaS - інфраструктура як послуга - уразливість даної моделі криється в ізоляції різних замовників в хмарі, яку забезпечує технологія віртуалізації. В даному випадку

віртуалізація повинна забезпечувати правильну сегментацію віртуальних машин клієнтів, що знаходяться на одній фізичній суті, а також необхідно забезпечити захист від підміни IP і MAC адресів клієнта, щоб у одного клієнта не було можливості скористатися чужим акаунтом.

2. SaaS - програмне забезпечення як послуга - для цієї моделі обслуговування характерні класичні для інтернет-додатків загрози: XSS-уразливість і вразливість, пов'язані з аутентифікацією (витік паролів). При такій моделі повинна дотримуватися сувора політика в галузі управління ідентифікацією та контролю доступу до додатків.

3. PaaS - платформа як послуга для розробки додатків - основною проблемою для даної моделі, також як для IaaS, є забезпечення ізоляції замовників, а також загрози, пов'язані з роботою через програмний інтерфейс, тобто ненадійне шифрування при передачі даних. В даному випадку необхідна сувора аутентифікація для ідентифікації користувачів, постійний аудит і дотримання конфіденційності.

Для успішного з'ясування «больових точок» систем віртуалізації і способів їх усунення або зниження їх значущості можна виділити наступні атаки:

1. Атака на віртуальну машину:
   - з іншої віртуальної машини;
   - на диск і файли конфігурації віртуальної машини;
   - на мережу реплікації віртуальних машин;
   - на мережу і систему зберігання даних містить файли віртуальної машини;
   - на засоби резервного копіювання віртуальної машини.
2. Атака на хост віртуалізації:
   - з фізичної мережі;
   - засобами скомпрометованого сервера управління віртуальною інфраструктурою;
   - на внутрішні сервіси гипервизора;
   - на агенти гипервизора від сторонніх виробників.
3. Атака на сервер управління віртуальної інфраструктури:
   - на ОС, яка забезпечує функціонування керуючих сервісів;
   - на СУБД сервера управління;
   - на базу облікових записів;
   - мережеві атаки на сервіс взаємодії і моніторингу з хостами віртуалізації.
4. Атака на ресурси хоста віртуалізації шляхом:
   - неконтрольованого зростання числа віртуальних машин;
   - некоректного планування розмежування пулів ресурсів;
   - некоректного планування зростаючих у міру заповнення віртуальних дисків віртуальних машин;
   - некоректного розмежування прав користувачів і груп віртуальної інфраструктури.

Крім цього, з точки зору організації віртуальної мережі виникає нове поняття як віртуальний комутатор, який забезпечує мережеву взаємодію віртуальних машин в межах одного хоста віртуалізації. Проблема віртуальних комутаторів полягає в непідконтрольності внутрішньомережевого трафіку, а також в можливості прослуховування всього мережевого трафіку між віртуальними машинами. В якості вирішення цієї проблеми прослуховування портів можливий такий варіант - організація мереж на базі віртуальних комутаторів, де тегування кадрів відбувається на рівні хоста віртуалізації ще до потрапляння пакетів в фізичну мережу [3].

Хмара представляє собою багатошарову структуру, де загальний захист системи дорівнює захисту найслабшого елементу в ній. Наприклад, успішна атака на міжмережевий екран або proxy-сервер, що стоїть на кордоні хмари і виходом в

Інтернет, заблокує доступ до всіх ресурсів, проте, зв'язки всередині неї будуть зберігатися. Ефективним захистом від функціональних атак буде використання для кожної частини хмари наступних засобів захисту: для proxy-серверу - ефективний захист від DDoS, для веб-сервера - контроль цілісності сторінок, для сервера додатків - екран рівня додатків, для систем управління базами даних - захист від SQL-ін'єкцій, для системи зберігання даних - правильно налаштовані програми резервного копіювання, а також розмежування доступу.

Віртуальна хмарна інфраструктура вимагає нового підходу до забезпечення безпеки інформації тому, що в існуючих інфраструктурах великими темпами успішно віртуалізуються різного роду інформаційні системи, проте методи і підходи захисту інформації при цьому використовуються поки ті ж, що передбачені для фізичних серверів. Тому контроль і управління хмарами - є основною проблемою безпеки.

На даний момент є декілька спеціалізованих систем захисту віртуальної хмарної інфраструктури, які можна розділити на наступні класи:

- програмні продукти для аналізу трафіку і запобігання вторгнень, що розроблені спеціально для віртуального середовища;
- програмне забезпечення для розмежування прав доступу до віртуальної інфраструктури;
- продукти для проведення аудиту віртуального середовища на предмет наявності помилок в конфігурації безпеки;
- продукти забезпечення безпечного, апаратно контрольованого підключення терміналів тонкого клієнта до віртуальної машини, що виконуються на сервері.

Таким чином, ефективне рішення щодо забезпечення інформаційної безпеки віртуальної хмарної інфраструктури повинно включати в себе використання віртуальних мереж і тунелів, стійкі алгоритми шифрування, розмежування доступу до порталу замовника з використанням різних методів фільтрації, захист периметру віртуального дата-центру, антивірусний захист віртуальних машин, захист від DDoS-атак.

Список літератури

1. Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації //Інформаційні технології та комп'ютерна інженерія: збірник тез доповідей науково-практичної конференції, м. Кіровоград, 4 грудня 2014 року. — Кіровоград: КНТУ, 2014. — С.164.

2. Ладигіна О.А. Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту// Інформаційна безпека держави, суспільства та особистості: Збірник тез доповідей Всеукраїнської науково-практичної конференції, 16 квітня 2015 року, - м. Кіровоград: КНТУ, - С. 45-47.

3. Бойко А,.Бердник А, Методы защиты виртуальной среды. Программный комплекс для проведения автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности, [Электронный ресурс] - Режим доступу: http://cyberleninka.ru/article/n/metody-zaschity-virtualnoy-sredy-programmnyy-kompleks-dlya-provedeniya-avtomatizirovannogo-audita-virtualnoy-sred