АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФРАСТРУКТУРІ ХМАРНИХ ОБЧИСЛЕНЬ

Коханевич Є.Г.
Науковий керівник – к.т.н., доцент Федюшин О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій, тел.702-14-25)
e-mail: yevhenii.kokhanevych@nure.ua, тел. (066) 189-79-17)

In this work the features of information security of cloud infrastructure are considered. Also we created a test environment using the OpenStack program, and simulates the work of cloud computing services to identify the major threats.

Then, we identified the main metrics with which you can identify the incident of information security in the cloud. In the end, a neural network was created that was capable of responding to information security incidents in accordance with data obtained from metrics.

Широке розповсюдження мереж з високою потужністю, низька вартість комп'ютерів та приладів збереження даних, а також масове впровадження віртуалізації, сервіс-орієнтованої архітектури призвело до дуже великого зростання хмарних обчислень. Хмарні обчислення – це модель забезпечення зручного доступу до обчислювальних ресурсів через мережу, які оперативно надаються та звільняються з мінімальними зусиллями з боку клієнта.

Але через те, що користувачі не мають доступу до роботи обладнання технологічної інфраструктури, яка їх підтримує, приватна інформація користувача фактично стає доступна третій стороні – провайдеру, окрім цього данні стають вразливими під час їх передачі по каналам зв'язку. Хоча великі постачальники і роблять все можливе для забезпечення високого рівня безпеки всередині хмари, але особливості побудови хмарної інфраструктури, використання технології віртуалізації та пов'язана з нею можливість порушення ізоляції віртуальних машин, а також паралельна обробка великих об'ємів інформації різних споживачів хмарних послуг, призводить до виникнення нових можливих загроз інформаційної безпеки, які будуть специфічними лише для хмарних обчислень.

На сьогодні провідними організаціями, що займаються питаннями безпеки в хмарі, є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, а також дві державні організації Європи та США: Європейське агентство мережної та інформаційної безпеки (ENISA) і Національний інститут стандартів і технологій (NIST). Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки в хмарі[1-3].

Найбільш поширена проблема інформаційної безпеки, яка виникає при роботі в хмарному середовищі, пов’язана з некоректною конфігурацією інфраструктури та не своєчасним реагуванням на інциденти, що виникають.

Метою даної роботи є реалізація ефективного засобу аудиту інформаційної безпеки в інфраструктурі хмарних обчислень та оперативного реагування у випадку виявлення потенційних загроз.

Під час виконання роботи було створено тестове хмарне середовище з допомогою інструменту OpenStack. В тестовій інфраструктурі була змодельована робота декількох споживачів хмарних послуг та проведений аналіз безпеки в середині кожної з них та їх вплив один на одного. В ході аудиту безпеки були визначені основні метрики, які дозволяють найбільш ефективно визначити інциденти інформаційної безпеки.

Наступним етапом роботи було розроблення ефективного засобу реагування на виникаючі загрози. Була створена нейронна мережа, яка здатна активно реагувати на інциденти інформаційної безпеки згідно з показниками метрик, які їй надаються. Таким чином, нейронна мережа здатна виконувати певні визначені дії по налаштуванні роботи інфраструктури у випадку отримання результатів метрик, що свідчать про виникнення чи існування певного інциденту в інформаційній безпеці даної інфраструктури. Робота нейронної мережі була реалізована згідно з алгоритмом, що детально описаний в [4].

Як результат ми отримали засіб оперативного реагування на інциденти та загрози інформаційної безпеки, що виникають в інфраструктурі хмарних обчислень. Ця система дозволяє забезпечити ефективний аналіз безпеки в інфраструктурі з врахуванням особливостей хмарних технологій та оперативні дії у випадку виявлення загроз інформаційній безпеці.

Список джерел:

1. Cloud Security Alliance “Treacherous 12: Top Threats to Cloud Computing” – 2016 [Electronic resource]. – URL: cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-deep-dive.

2. European Union Agency for Network and Information Security “Cloud Security Guide for SMEs” – 2015 [Electronic resource]. – URL: www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

3. National Institute of Standards and Technology “Guidelines on Security and Privacy in Public Cloud Computing” – 2011 [Electronic resource]. – URL: nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf.

4. Сенцова А. Ю. Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений: дис. канд. техн. наук: 05.13.19 / Сенцова Алина Юрьевна. – Уфа, 2016. – 208 с.