УДК 004.056:355.451]:004.75

БЕЗПЕКА ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ХМАРНИХ СЕРВІСІВ

Белозьоров С. Ю.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-301-66-25

The presented work is devoted to the analysis of modern intrusion detection
The work is devoted to the analysis of methods of ensuring information security of telecommunication networks using cloud services. Data center security in a cloud computing environment must be multi-layered. It uses: next-generation NGFW network virtual appliances, WAF web security applications, continuous monitoring, encryption, two-factor authentication, and basic anti-virus software. It is also advisable to use IDS/IPS intrusion detection and prevention systems. One of the methods of effective protection is to use the possibilities of providing protection in the cloud services themselves.

Хмарні обчислення поступово стають однією з найпоширеніших інформаційних технологій.

І, як наслідок, спостерігається значне зростання кількості мережевих атак.

По-перше, загрозам піддаються різні програмні продукти елементів хмари, впровадження в які дозволяють зловмиснику як отримати доступ до системи, так і порушити її функціональність.

По-друге, вразливість хоча б одного елемента хмарної інфраструктури у разі проведення на неї мережевої атаки дає змогу заблокувати всю систему.

По-третє, зловмисник спроможний не тільки забезпечити собі доступ до даних, що зберігаються та оброблюються в хмарному сервісі, а й підкорити його собі таким чином, що хмара та її ресурси функціонуватимуть на користь порушника. Крім того, реалізується можливість здійснювати мережеві атаки по відношенню до конкретних користувачів. Внаслідок реалізації подібних загроз зловмисник може здійснювати такі традиційні атаки на користувачів веб-додатків, як перехоплення мережевих сесій, крадіжка паролів тощо.

Безпека центру обробки даних у середовищі хмарних обчислень має бути багаторівневою, що включає такі аспекти: контроль доступу, ідентифікація працюючого персоналу, моніторинг системи, миттєве сповіщення про вторгнення і т.д.

Щоб захистити хмару від вторгнення, вірусних програм та витоку даних, необхідно насамперед налаштувати контроль доступу. Завдання полягає в тому, щоб не просто налаштувати доступ для користувачів –

вибрати логін та пароль, а не допустити вторгнення ззовні. Для цього використовуються: мережеві віртуальні пристрої Firewall, програми захисту веб-інтерфейсу, безперервний моніторинг.

Важливими елементами захисту також є: шифрування, двофакторна автентифікація та базове антивірусне програмне забезпечення. Вони мають бути реалізовані провайдером.

Основний спосіб коректно відфільтрувати відомості та проконтролювати доступ до ресурсів – це використання багатофункціональних Firewall (брандмауерів). Сучасні Firewall наступного покоління (NGFW) відрізняються інтегрованими функціями безпеки для хмарних сервісів: наявність функції NAT/PAT, глибока перевірка пакетів з підписом поведінки.

Доцільно також використовувати системи виявлення та запобігання вторгненням IDS/IPS, спеціалізовані веб-елементи управління - правила WAF (Web Application Firewall).

Один із методів ефективного захисту - використання можливостей надання захисту у самих хмарних сервісах. У разі використання хмарних технологій PaaS та SaaS, ряд елементів безпеки може надати постачальник. У випадку IaaS (Інфраструктура як послуга) можна організувати повноцінну систему захисту і забезпечити деталізацію та вибір елементів керування захистом.

Для ефективного захисту інформації у хмарі розгортається велика кількість списків контролю доступу у всіх можливих точках входу. Основна проблема – організація управління правилами. Ці питання вирішені розробниками хмарних сервісів Amazon AWS та Microsoft Azure.

Microsoft Azure для захисту даних у хмарі може забезпечити:

• контроль доступу через групи безпеки мережі (NSG);
• балансування навантаження;
• WAF, але без великого набору керованих правил та централізованого керування ними;
• єдиний міжмережевий екран між мережею та Інтернетом;
• кілька брандмауерів на різних рівнях;
• ізоляцію мереж.

Можна також використовувати Amazon AWS. У порівнянні з Microsoft Azure Amazon AWS має більш ефективні механізми захисту, але є складним в налагоджненні і коштує більше.

Список використаних джерел:

1. Microsoft. Azure. Products. Security. Protect your enterprise from advanced threats across hybrid cloud workloads. https://azure.microsoft.com/en-us/

2. Amazon. AWS solutions. Cloud security software. https://aws.amazon.com/marketplace/solutions/security/?nc2=h_ql_mp_sol_sec