ПІДТРИМКА БЕЗПЕКИ МЕРЕЖІ В ПРОЦЕСІ РОЗГОРТАННЯ ХМАРНОГО СЕРЕДОВИЩА НАВЧАЛЬНОГО ЗАКЛАДУ

Гриб'юк О.О.
Інститут інформаційних технологій та засобів навчання НАПН України,
Національний педагогічний університет імені М.П.Драгоманова
olenagrybyuk@gmail.com

Анотація

Наводяться фактори ефективності організації системи безпеки мережі в хмарному середовищі з використанням ядра ОС Linux. Розглядаються шляхи підтримки безпеки мережі в процесі розгортання хмарного середовища навчального закладу, специфікація розгортання системи, долучення додаткового хмарного провайдера, динамізація балансувальників навантажень, монтування пристроїв блочного зберігання та ефемерних пристроїв з використанням зашифрованої файлової системи та віртуалізація серверів на ОС Linux, експериментування з конфігураціями і перебудовою образів комп'ютера.

Відмінність між традиційними центрами опрацювання даних і хмарним середовищем полягає у фізичному розташуванні навчальних матеріалів на серверах, що належать не користувачеві (навчальному закладу), а сторонній організації. Доцільність використання послуг аутсорсингу та послуг провайдера частково подолали проблеми між фізичною інфраструктурою ІКТ та хмарним середовищем.

Важливою проблемою є обмеження доступу до навчальних матеріалів (даних), наприклад, неспроможність обраного хмарного провайдера захистити компоненти пропонованої ним інфраструктури. Необхідними мірами є шифрування даних та виконання віддаленого резервного копіювання (в тому числі шифрування резервних копій та мережевих комунікацій на іншому хмарному сервісі, шифрування мережевого трафіка разом з web-трафіком). Рекомендується долучити додаткового хмарного провайдера для виконання автоматизованих процедур резервного копіювання, забезпечуючи гарантоване відновлення даних та їх історію навіть за умови фізичного знищення обладнання хмарного провайдера. Необхідне налаштування рівня контролю щодо використання даних в

хмарному середовищі та центрі опрацювання даних. При формуванні наборів даних для резервного копіювання рекомендується шифрування з використанням криптостійкого алгоритму (*Pretty Good Privacy*).

Важливою під час розгортання хмарного середовища є можливість створення ефемерних пристроїв зберігання даних при використанні віртуального сервера, хоча в середовищі відсутність шифрування ефемерних пристроїв становить загрозу у зв'язку із затиранням ефемерних пристроїв нулями при завершенні роботи системи.

Безпечність зберігання та використання даних в хмарному середовищі полягає у монтуванні пристроїв блочного зберігання та ефемерних пристроїв з використанням зашифрованої файлової системи (*encrypted filesystem*). Доцільне зберігання паролів захисту системи в незашифрованій кореневій файловій системі, а не в хмарному середовищі. Процес запуску віртуального сервера з використанням паролів доступу проілюстровано у проекті.

Специфікація розгортання системи в хмарному середовищі можлива за рахунок реалізації змішаної архітектури, що складається з фізичних елементів та деяких віртуальних. В хмарній інфраструктурі змішаного середовища не зберігаються конфіденційні дані, оскільки їх опрацювання виконується на серверах підконтрольного користувачеві фізичного ЦОД. Захист периметра сегментів мережі здійснюється з використанням брандмауера (*firewall*). За допомогою брандмауера захищається зовнішній периметр мережі, при цьому пропускаються тільки трафіки *http, https, ftp*. Брандмауер розглядається як пара механізмів: один для блокування передачі даних, інший – для їх запуску. Ядро *ОС Linux* має вбудований екран *netfilter* . Для його налаштування і управління поставляється програмний пакет *iptables*. Цей пакет окрім файлів документації та модулів включає *iptables, iptables-save, iptables-restore.* Управління системою *LIDS (Linux Intrusion Detection/Defence System)* - додатком до ядра *ОС Linux* здійснюється за

допомогою програми *lidsadm* у двох режимах: режим налаштування правил доступу і режимі введення команд адміністрування. *AIDE* – розширене оточення виявлення вторгнення. Основне призначення – виявлення зміни файлів, їх атрибутів, прав доступу, користувачів, розміру, кількості посилань на файл та інших параметрів файлу. Одразу після встановлення і налаштування необхідних сервісів і програм в *Linux*, але перед підключенням до мережі, адміністратор повинен створити базу *AIDE(Advanced Intrusion Detection Environment)***.** *Linux ACLs* - це набір заплаток для ядра *ОС* і програм для роботи з файловою системою і декількох додаткових програм, що дають можливість встановлювати права доступу до файлів не тільки для користувача-власника і групи-власника, але і для будь-якого користувача групи. Список розширеного контролю доступу існує для кожного файлу в системі і складається із 6 компонентів: *ACL_USER_OBJ, ACL_GROUP_OBJ, ACL_OTHER, ACL_USER, ACL_GROUP, ACL_MASK.* Між захищеним сегментом мережі і зовнішнім периметром знаходяться проміжні системи – балансувальники навантаження, через які трафік спрямовується в спеціальну область, де знаходяться сервери ПЗ. Запити направляються до бази даних через інший брандмауер у внутрішню захищену мережу з внутрішніми базами конфіденційних даних. Структура використовується для отримання доступу до даних із збільшенням рівня секретності, причому організовується кілька периметрів захисту мережі за допомогою брандмауерів. При компрометації внутрішнього сервера в межах сегмента автоматично надається доступ до інших серверів в цьому ж сегменті, що є недоліком такої інфраструктури. В хмарному середовищі не існує периметрів і сегментів мережі. Всі віртуальні сервери знаходяться в мережі на одному рівні, а управління трафіком здійснюється засобами груп безпеки (*security*). Ефективність організації системи безпеки мережі в хмарному середовищі залежить від багатьох факторів. На кожному віртуальному сервері доцільно запускати один мережевий сервіс та сервіси для адміністрування.

Зосередження на одному сервері кількох сервісів може призвести до виникнення векторів вірусних атак. Навіть при обмеженні використання балансувальника навантаження рекомендується використання зворотного проксі-сервера (*reverse proxy*). За допомогою зворотного проксі-сервера ретранслюються запити користувача із зовнішнього середовища на сервери у внутрішній мережі. Зазвичай reverse proxy розташовуються перед *web*-серверами і використовуються в ролі брандмауера на прикладному рівні для балансування навантаження в мережі між кількома *web*-серверами та підвищення їх безпеки.

Для налаштування автоматизації усунення проблем безпеки в мережі рекомендується використання динамічної природи хмарного середовища. Мережеві системи виявлення вторгнень призначені для попередження і відображення вірусних атак. Виявлення вторгнення в мережу здійснюється шляхом маршрутизації усього трафіка через систему, що використовується для його аналізу, або відповідно шляхом пасивного моніторингу трафіка з одного комп'ютера відповідної локальної мережі. В хмарному середовищі додаткова система виявлення вірусних атак ефективна завдяки можливостям виявлення та знешкодження шкідливого вмісту мережевих пакетів.

Оригінальним підходом для запуску та використання віддаленого сервера NIDS на балансувальнику навантажень є його встановлення на сервер перед мережею, завдяки чому здійснюється моніторинг трафіка. Виявивши спосіб компрометації балансувальника навантажень, вірусний атакуючий захоплює контроль над балансувальником навантажень та отримує можливість призупинення процесу виявлення вторгнень. Альтернативний підхід полягає в реалізації системи виявлення вторгнень на сервері в позиції за балансувальником навантажень, що функціонує як проміжна точка між балансувальником навантажень та іншими компонентами системи. В хмарному середовищі розгортання ПЗ з підтримкою системи безпеки передбачає встановлення поновлень безпеки,

тестування результатів, перезавантаження усіх віртуальних серверів, мінімізуючи операції в хмарі, унеможливлюючи виникнення помилки.

В хмарному середовищі можливе експериментування з конфігураціями і перебудовою образів комп'ютера. Дібравши конфігурацію для конкретного сервісного профілю, можна попередньо підсилити захист системи перед розгортанням образу в хмарному середовищі. Мережеві системи виявлення вторгнень на рівні хосту (HIDS) функціонують аналогічно до антивірусних систем та за їх допомогою додатково досліджуються системи на всі ознаки компрометації та подаються повідомлення про всі випадки зміни системних сервісів та файлів ОС. В хмарній інфраструктурі обирається централізована конфігурація для розробки профілю безпеки підвищеного рівня із високим ступенем захисту сервісів за принципом «один сервер – один сервіс». Сегментація даних відповідно до рівнів конфіденційності є основним засобом мінімізації впливу вірусної атаки на продуктивність системи. Рекомендується забезпечувати доступ до віртуальних серверів динамічним наданням відкритих ключів на цільовий сервер, передаючи паролі через адміністративний інтерфейс, а не за рахунок облікового запису користувача. При зміні користувача рекомендується будувати інший образ комп'ютера із необхідними новому користувачу змінами.

Ґрунтовний підхід полягає у використанні засобів управління хмарною інфраструктурою, або розробці необхідного інструментарію, завдяки чому зберігаються облікові дані користувачів за межами хмарної інфраструктури та з'являється можливість динамічно додавати/вилучати облікові записи користувачів на хмарні сервери. Такий підхід потребує створення і запуску адміністративного сервісу на кожному хості. В хмарному середовищі при компрометації доцільне копіювання кореневої файлової системи на один із томів, копіювання томів при зупинці сервера та його заміні.