УДК 004.75

ХМАРНІ ТЕХНОЛОГІЇ БЕЗПЕКИ

Комiссар Д. О., Луппол Є. Ю.

CLOUD SECURITY TECHNOLOGIES

Komissar D. , Luppol I.

У цій статті буде розглянуто, як програмне забезпечення для комп'ютерної безпеки може захистити від шкідливого ПЗ, при чому виносячи частину функціоналу в «хмару». Також багато уваги приділяється захищеності та швидкодії такої системи.

Ключові слова: *Хмарні обчислення, антивірусні технології, інформаційна безпека.*

Вступ. Персональні комп'ютери, мережі і Інтернет існують менше 25 років, але вони глибоко увійшли у повсякденне життя. Комп'ютер, що не має доступу до мережі Інтернет має досить обмежену галузь застосування. В той же час обличчя комп'ютерної безпеки теж змінилося: загрози, які раніше поширювались за допомогою носіїв даних, зараз переважно потрапляють до комп'ютерів з мережі.

Наріжним каменем традиційної комп'ютерної безпеки завжди було антивірусне програмне забезпечення – автономне ПЗ, яке оновлюється і може визначити, чи є шкідливою будь-яка інша програма. З тих пір, як у 1980-х роках з'явилися перші антивіруси, вони багато в чому змінились, але основні принципи їх функціонування залишились непорушними. Але перед обличчям різких змін в застосуванні і поширенні мережевих технологій, комп'ютерна безпека повинна також принципово змінюватись.

Останні тенденції в сфері обчислювальних технологій направлені на рознесення навантаження та безобмежений доступ до ресурсів, що класично забезпечується хмарними технологіями. Під хмарними технологіями безпеки розуміється будь-який вид комп'ютерної безпеки, який активно взаємодіє з зовнішніми віддаленими серверами. Ця взаємодія може, наприклад, забезпечувати зворотній зв'язок від баз даних, репутаційних систем, чорних і білих списків, керованих послуг и т.п. Ця швидка відповідь може дати антивірусу необхідну інформацію, щоб визначити зловмисну поведінку.

Звичайні антивіруси проти хмари. Останнім часом, вірусні атаки, які підживлюються в основному фінансовими стимулами, значно зросли за частотою. Це, звичайно, означає, що оновлення системи захисту теж повинно відбуватися частіше. Таким чином, антивірусні компанії намагаються зменшити час між випуском оновлень для своїх продуктів. Але логічно було б зробити висновок, що найкращий захист той, який доставляється миттєво. Сучасні мережі стають все швидше і швидше, тому тепер можна виконувати антивірусні перевірки без порушення нормальної роботи комп'ютера і домогтися майже миттєвої доставки.

Для традиційних антивірусних рішень захист комп'ютера від ШПЗ відбувається за 4 кроки: винайдення ШПЗ, створення сигнатури, розсилка та застосування оновлення. Звичайно, затримки можуть потенційно виникати на кожному з цих кроків. Хмарні технології дозволяють забезпечити значно швидшу реакцію.

Чим швидше розгортається захист, тим кращу безпеку отримують користувачі. Але крім швидкого розгортання захисту, хмарні технології можуть вирішити ще одну проблему – швидко зростаючі антивірусні бази в системі, що спричиняє уповільнення роботи комп'ютера. З кривої зростання загроз можна зробити висновок, що захист буде вимагати збільшення об'єму використаної пам'яті та місця на диску. В той же час ШПЗ стає недовговічними (наприклад, спам). Постійне збільшення кількості унікальних загроз та зменшення часу життя загроз також означає, що більшість антивірусних оновлень ніколи не буде використана, тому що комп'ютер не буде стикатися з цими загрозами.

Один з варіантів вирішення цих проблем – зберігати останні оновлення захисту на хмарних серверах, до яких клієнтське програмне забезпечення може звертатися при необхідності. Це рішення може обмежити швидке зростання баз локального антивірусного програмного забезпечення. У якійсь точці в майбутньому ці бази могли б навіть почати зменшуватись, у зв'язку з тим, що більшість захисного контенту рухається до хмар.

Швидкодія Хмар. Для анти-спам програмного забезпечення порівняно легко провести онлайн-перевірку, скажемо, домену, який зустрічається як посилання в електронній пошті. Невелика затримка доставки електронної пошти не буде порушувати нормальну роботу комп'ютера, тому що перевірка відбувається до того, як лист буде доставлений, а пошта не доставлятися миттєво. Антивірусне програмне забезпечення у набагато більш складній ситуації: якщо користувач запускає програму, будь-яка помітна затримка зменшує продуктивність. Якщо

технологія безпеки, що базується на хмарному підході, буде робити помітні затримки, то вона просто не буде використовуватись.

В той же час, якщо хмарні технології не можуть забезпечити швидкість порівняну з локальним антивірусним скануванням, тоді їм буде дуже важко конкурувати з традиційними антивірусами. Якщо, наприклад, антивірусне сканування програми займає 50 мс, тоді швидка хмарна перевірка повинна теж досягати швидкості такого порядку (передбачається, що локальна мережа не створює відчутних затримок).

На щастя, існує багато стратегій, які можна застосувати, для уникнення затримок:

- списки виключень
- застосування пошарового хмарного сканування
- затримки пов'язані з хмарним скануванням можна компенсувати за рахунок зменшення використання ресурсів локальної обчислювальних машини.

Логічний спосіб ввести захист базований на хмарах – об'єднати його з існуючим антивірусним ПЗ. У такого підходу величезні переваги. Антивірус має існуючу інфраструктуру, щоб доставляти оновлення для всіх серверів і робочих станцій, що знаходяться під захистом. Цей механізм не настільки швидкий, як повинен бути, щоб протидіяти швидкому поширенню ШПЗ, але антивірусні оновлення можуть бути успішно використані для базового захисту від найбільш чисельних і постійних загроз. Крім того, ці оновлення можуть також доставляти хмарному клієнту правила і білі списки, гарантуючи, що загальні чисті файли не будуть перевірятися. Простий білий список може зменшити кількість мережевого сканування на кілька порядків. Таким чином, традиційне антивірусне оновлення може бути застосоване і для хмарних технологій, дозволяючи швидке і безшовне прийняття нової технології, оскільки необхідна інфраструктура вже створена.

Інша перевага застосування хмарної технології до антивірусних сканерів полягає в тому, що вони вже здатні перевіряти вхідні об'єкти на багатьох рівнях. Наприклад, сканери мають всі необхідні функції для перевірки електронних листів і додатків до них, посилань, об'єктів, які завантажуються з мережі Інтернет, програм що самі виконують завантаження контенту. Важливо перевірити програми, які потрапляють до системи через будь-який з цих шляхів. Якщо хмарні перевірки виконуються для всіх цих вхідних точок, то затримки, викликані додатковими мережевими перевірками можна зменшити. Це досягається за допомогою того, що будь-яка комп'ютерна система містить і використовує багато тисяч програм щоденно, тоді як тільки невелика кількість програм зазвичай додається (не беручи до уваги, звичайно, виключні ситуації, такі як, наприклад, впровадження пакетів оновлення або масоване встановлення програмного забезпечення; але навіть у таких ситуаціях лише невелика кількість нових пакетів потребує ретельної перевірки, бо більшість з них вже буде знаходитись в білих списках).

Щоб затримки були малими, хмарні технології повинні бути розроблені та впроваджені, з основною ідеєю - швидкодія. Кількість, розмір і частота переданих і отриманих пакетів повинна бути настільки малою, наскільки це можливо. Щоб підтримувати високошвидкісну роботу, хмарні сервери повинні також бути швидкими, з низькими затримками, відмовостійкими і мати відповідне географічне положення.

Офлайн захист. З'єднання антивірусного ПЗ з хмарною технологією має ще одну перевагу: якщо остання не працює (наприклад, коли комп'ютер не підключений до мережі Інтернет), тоді захист перетворюється на традиційний. Враховуючи те, що більшість загроз приходить з мережі, втрата з'єднання може не підвищувати рівень ризику.

Антивіруси і хмарні технології можуть працювати, як ефективний симбіоз. Антивірус буде забезпечувати довготривалий захист від постійних загроз (наприклад, від розповсюджених шкідливих програм, таких як віруси, черв'яки та троянські програми), тоді як хмарна частина буде забезпечувати швидкий захист від недовговічних спалахів іншого ШПЗ.

Трафік і затримки. Дуже активний клієнт в хмарних антивірусних рішеннях може споживати велику кількість мережевого трафіку. Такий клієнт також викликає більшу завантаженість серверів, що, в свою чергу, призводить до зменшення загальної швидкості відповіді іншим клієнтам. Таким чином, краще мінімізувати кількість даних, які передаються між клієнтом і сервером. Легкі протоколи мають перевагу – UDP замість HTTP, який вимагає синхронізації перед будь-якою передачею даних, або HTTP замість HTTPS, який повинен передавати захищену інформацію, що, безумовно, тільки додає накладних витрат.

Щоб зменшити вимоги до трафіку, можна використовувати декілька підходів:

- хмарне рішення може бути об'єднане з традиційним антивірусом, який буде фільтрувати всі відомі загрози. Таким чином, зменшиться кількість перевірок по мережі.
- хмарний клієнт може використовувати локальний білий список, щоб уникати перевірки відомих файлів.
- кешування відповідей допоможе обійтися без повторних запитів.

Затримка між географічно віддаленими серверами повинна забезпечувати досягнення поставлених цілей. Як правило, запити до хмар не повинні займати більше часу, ніж ретельне локальне сканування файлу на диску.

Затримка може збільшитись, коли сервер перевантажений. Це викликає ще один характерний ризик хмарних технологій – організовану розподілену атаку (DDOS) на сервер. Було б логічно очікувати, що зловмисники спробують обійти хмарний захист найпростішим шляхом, дати команду бот-мережам запустити DDOS-напад. Для зменшення ефективності такої атаки можна фільтрувати небажаний трафік або використовувати розподілену мережу серверів (наприклад, інфраструктура Akamai). В якійсь мірі, географічний розподіл серверів для досягнення низької затримки вже значно підвищує стійкість хмари до таких атак.

Але крім мінімізації споживання трафіку і максимізації швидкості роботи необхідно переконатись, що комунікації є безпечними.

Безпека. «Хмарність» антивірусних рішень відкриває для зловмисників деякі можливості маніпулювати нормальною роботою системи. Зловмисники можуть:

- перехоплювати дані, які передаються від клієнта до сервера
- перехоплювати відповідь сервера клієнту
- запускати DDOS атаку на сервер.

Перехоплення вихідних даних клієнта (наприклад, аналізаторами трафіку) навряд чи призведе до порушення конфіденційності, тому що інформація, що передається (якщо антивірусний продукт відповідає чинному законодавству і прийнятим стандартам) не повинна містити конфіденційних даних. Однак, інколи сам факт, що така передача відбувається може виявитися важливим (наприклад, як показник того, що система, швидше за все, буде скомпрометована). Можна прийняти деякі міри для того, щоб мінімізувати ризик цього, такі як використання DNS протоколу. В цьому випадку всі зовнішні комунікації стають анонімними. Джерелом стає DNS сервер, а не індивідуальні клієнти, тому IP адреса клієнта не буде доступна ззовні.

Захист клієнтів від підроблених відповідей повинен бути одним з ключових питань. Якщо інфраструктура чиста (із відповідними брандмауерами і належним фізичним захистом), то все одно повинна бути передача даних між клієнтом і сервером.

Найгірший сценарій – якщо хмара викликає помилкову тривогу, коли для безневинного файлу генерується хибно-позитивна («знайдене шкідливе ПЗ») відповідь. В такому випадку буде відбуватися дія за замовчуванням для антивірусного продукту. Зазвичай, з'явиться спливаюче вікно «видалити, або відправити на карантин». Якщо зловмисник буде спроможний підмінити результат сканування для будь-якого важливого системного файлу (наприклад, winlogon.exe або ntodkernel), ще може мати катастрофічні наслідки. Цього можна уникнути, якщо дані, які приходять від сервера, будуть мати цифровий підпис. Клієнт може перевірити підпис і не сприймати будь-які неправильні відповіді та спроби підмінити дані. Ще один спосіб - використовувати шифрування, таке як SSL, для даних, які передаються між клієнтом і сервером під час TSP/IP сесії (HTTPS протокол робить це автоматично). Цей метод повільніший, але також вирішує проблему підміни даних.

Організація Cloud Security Alliance (CSA) і корпорація Hewlett-Packard представили документ "Top Threats to Cloud Computing V1.0" ("Головні загрози розвитку хмарних обчислень"). Він був складений за результатами проведеного дослідження і адресований як провайдерам хмарних сервісів, так і їх користувачам. Основними категоріями загроз виявились такі:

1) зловживання і нечесна гра при використанні хмарних ресурсів;
2) небезпечні інтерфейси та API;
3) зловмисники з числа інсайдерів;
4) спільне використання ресурсів;
5) втрата або витік даних;
6) несанкціоноване використання облікового запису або сервісу;

Зупинимося більш докладно на другому пункті – «небезпечні інтерфейси та API». Для роботи з хмарними сервісами провайдери надають клієнтам спеціальні програмні інтерфейси. Від того, як в цих інструментах реалізовані заходи забезпечення інформаційної безпеки (аутентифікація, контроль доступу, шифрування, моніторинг активності), багато в чому залежить безпека і самого сервісу. Проблема ускладнюється у випадку, якщо на базі хмарних ресурсів одного провайдера стороння компанія будує і пропонує додаткові послуги і відповідальність перед замовником за заходи безпеки виявляється розподіленою. Так що перед тим, як почати користуватися хмарними сервісами, слід переконатися в безпеці запропонованих провайдером інструментів, щоб не наражати компанію на невиправдані ризики.

Конфіденційність. Хмарне сканування може бути реалізоване багатьма способами. Воно може мати або не мати проблем з конфіденційністю. Наприклад, якщо клієнт передає серверу тільки хеш об'єкту (або частину об'єкту), тоді неможливо виділити ніяку приватну інформацію.

З іншого боку, клієнтський додаток, розроблений зі слабким розумінням проблем конфіденційності, може передавати геть усе: весь

просканований об'єкт, імена папок або IP та MAC адреси комп'ютера. Оскільки MAC адреса – це унікальне число, яке ідентифікує мережеву карту, то він може бути використаний для визначення конкретного комп'ютера. Передача такої інформації буде грубим порушенням конфіденційності, тому що файли, що передаються, можуть містити не тільки персональні дані, але також фінансову або секретну інформацію. Всі ці дані можуть бути пов'язані з конкретним комп'ютером за допомогою IP та MAC адрес.

Будь який постачальник антивірусного ПЗ має вибрати, яку інформацію передавати. Вони не повинні передавати будь-які дані, які можуть ідентифікувати людину (такі як MAC адреса). Передавитись повинно якомога менше інформації – необхідний мінімум для заданої мети. Інформація, що передається повинна бути анонімною.

Необхідно підкреслити, що тип протоколу передачі даних має пряме відношення до рівня конфіденційності. Наприклад, дані, що передаються по DNS-протоколу, спочатку потрапляють до локального DNS сервера (для корпорацій це буде внутрішній DNS, а для домашніх користувачів – DNS інтернет-провайдера), який в свою чергу зв'язується з сервером хмари. Цей захист локальним DNS сервером гарантує, що сервер хмари ніколи не бачить IP адресу клієнта. Все, що цей сервер може побачити – це IP адресу DNS сервера. Він, в свою чергу, може використовуватись багатьма тисячами клієнтів, тому персональна ідентифікація стає неможливою.

Якщо використовується TCP/IP зв'язок (наприклад, HTTP або HTTPS протоколи), тоді сервер має піклуватися, щоб IP адреси не використовувались не за призначенням. В ідеалі, вони повинні бути переведені у географічні дані, які будуть зберігатись замість IP адрес. Іншими словами, якщо вхідна інформація не повністю анонімна, серверне ПЗ має миттєво закривати ці пробіли.

В цілях безпеки надзвичайно важливо перевіряти шляхи до файлів, їх імена, атрибути (такі як цифровий підпис і автор) та інше. Ця інформація практично ніколи не може ідентифікувати людину, але в деяких випадках це можливо. На щастя, більшість сучасного ШПЗ спираються на код, що існує в файлах виконуваного типу. Передача атрибутів таких об'єктів безпечна з точки зору конфіденційності, тому що ці програми віртуально ніколи не містять ніяких приватних даних та не відкривають імені файлу. В той же час, треба максимально обережно витягувати атрибути з інших типів файлів, які передаються в хмару, особливо документи з вільним контентом (такі як DOC, DOCX, PPT, XLS і PDF).

Клієнт хмари має завжди шифрувати будь-яку інформацію, що він передає. Якщо дані не зашифровані належним чином, вони можуть бути перехоплені та переглянуті зловмисниками. Вже зазначалося, що таке перехоплення може мати наслідки для безпеки, а саме сприяти підміні відповідей від сервера та аналізу слабких місць у мережі. Але якщо до того ж передаються ще й конфіденційні дані, це може призвести також до розкриття імен людей, їх облікових записів та іншого.

Всі постачальники антивірусного ПЗ, які використовують хмарні технології, повинні опублікувати відповідні положення про конфіденційність та дотримуватись їх.

Проблеми тестування. Належне тестування традиційних антивірусних рішень дуже проблематичне, і воно стає все тяжче у зв'язку зі зростаючою їх складністю. Тестування хмарних технологій або комбінацій антивірусного та хмарного захисту ще складніше завдання.

Тести зазвичай працюють із «замороженими» продуктами і наборами зразків, так що результати є відтворюваними, повторюваними та підлягають перевірці. На жаль, не можна використовувати такий же підхід для хмарних рішень, тому що воно не може бути заморожене. Серверна сторона завжди буде динамічною і, будучи поза контролем тестера, не може бути зупинена. Отже, тестове середовище також стає досить «рухомим». Результати не можуть бути відтворені повторно, і шанси знайти помилки у тестах значно знижуються. З точки зору тестера, це еквівалентно введенню «чорного ящика» в тесті, і найгіршим є те, що чорний ящик може містити людей і третіх сторін (наприклад, інтернет-провайдерів). З іншого боку, розробники продуктів, що тестуються, можуть розглядати ці тести, як ненадійними і підозрілими, тому що ніщо не може бути відтворене.

Тестування хмарних антивірусних рішень тільки починається, тому ще нема загальноприйнятих методологій. Головна ідея проведення таких тестів – запускати антивірусні продукти на тривалий час з різних діапазонів IP адрес та географічних регіонів. Періодично можна отримувати середні результати такого тестування. Наприклад, середня затримка відповіді і середній рівень виявлення загроз за останній місяць можуть бути опубліковані щодня. Такий статистичний підхід повинен вирівняти короткострокові коливання, пов'язані з синхронізацією публікації особливих правил захисту, затримками на рівні інтернет-провайдера, тимчасовим навантаженням на сервер і т.д.

Переваги та недоліки хмарних антивірусів

Переваги:

- Дуже тонкий клієнт. Це означає дуже низьку витрату ресурсів клієнтом та меншу кількість вразливостей.
- Можливо, кращий рівень виявлення загроз, за рахунок використання більш ніж одного антивірусного ядра.

Недоліки:

- Проблеми трафіку роблять цей продукт непридатним для загальних цілей в недалекому майбутньому. Однак, продукт можна успішно використовувати в локальних мережах.
- Питання конфіденційності, особливо коли скануються не виконувані типи файлів, такі як документи і скрипти.
- Локальне кешування може викликати проблеми з оновленнями антивірусних баз. Крім того, безпечний механізм кешування включає в себе виконання безпечного алгоритму хешування по всьому файлу, який , як правило, повільніший, ніж сканування файлу локально.
- Використання більш ніж одного антивірусного ядра означає більше проблем з помилковими тривогами. Тим не менш, продукт може бути налаштований на видачу попереджень тільки тоді, коли вказане число антивірусних ядер повідомлять про те, що файл небезпечний.

Взагалі слід відрізняти типи захисту що надається одному віддаленому клієнту в гетерогенній мережі або захист, скажімо, корпоративної мережі, що може давати зовсім інші можливості, та матиме відповідні вимоги з конфіденційності та надійності, але це тематика для наступних досліджень.

Висновки. Використовуючи хмарні технології, клієнти можуть не тільки зменшити період «незахищеності» (від днів або годин до секунд), а ще й отримати набагато кращий захист. Крім того, антивірусні продукти можуть стати «легшими», тому що вони не потребують наявності і оновлення мільйонів сигнатур вірусів, більшість з яких ніколи не буде використана. Хмарні технології, однак, мають ризики, в основному пов'язані з конфіденційністю, але їх можна контролювати. Загалом, переваги хмарної системи занадто великі, щоб відмовлятися від неї.

Література

1. Muttik, C. Barton : Cloud security technologies. *McAfee Avert Labs, Alton House, Gatehouse Way, Aylesbury, Herts HP19 8YD, UK.*

2. M.Chiriac: Tales from cloud nine. *BitDefender, 24 Preciziei Blvd, West Gate Park, Building H2, Bucharest, Romania.*

3. И. Лапинский: Семь угроз развитию облачных вычислений. *PC Week/RE №12 — 13 (714 — 715) 6 — 19 апреля 2010.*

References

1. Muttik, C. Barton : Cloud security technologies. McAfee Avert Labs, Alton House, Gatehouse Way, Aylesbury, Herts HP19 8YD, UK.

2. M.Chiriac: Tales from cloud nine. BitDefender, 24 Preciziei Blvd, West Gate Park, Building H2, Bucharest, Romania.

3. I. Lapinskij: Sem' ugroz razvitiju oblachnyh vychislenij. PC Week/RE №12 — 13 (714 — 715) 6 — 19 aprelja 2010.

Комиссар Д. О., Луппол Е. Ю.

ОБЛАЧНЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

В этой статье будет рассмотрено как программное обеспечение для компьютерной безопасности может защитить от вредоносного ПО, при этом вынося часть функционала в «облако». Также много внимания уделяется защищенности и быстродействию такой системы.

Ключевые слова: *Облачные вычисления, антивирусные технологии, информационная безопасность.*

Komissar D., Luppol I.

CLOUD SECURITY TECHNOLOGIES

In this article we shall look at how computer security software can protect against malware whilst using knowledge stored on servers in the Internet cloud. Also, a lot of attention paid to self-security and speed of the system.

Keywords: *Cloud computing, anti-malware technologies, information security.*

Комісар Д. О., Луппол Є. Ю. – Національний технічний університет України «Київський політехнічний інститут»

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.