УДК 004.56
Г. Шимчук, О. Голотенко, Р. Золотий,
(Тернопільський державний технічний університет імені Івана Пулюя, Україна)

ОСНОВНІ ПРОБЛЕМИ ТА ЗАГРОЗИ ХМАРНОЇ БЕЗПЕКИ

УДК 004.56
G. Shymchuk, O. Holotenko, R. Zoloty

USE THE MAIN PROBLEMS AND THREATS OF CLOUD SECURITY

Майже кожна організація різною мірою використовує хмарні обчислення у своєму бізнесі. Однак із запровадженням хмари виникає необхідність переконатися, що стратегія хмарної безпеки організації здатна захистити від найпоширеніших загроз безпеці хмари.

Неправильна конфігурація параметрів безпеки хмари є основною причиною витоку хмарних даних. Стратегії керування хмарною безпекою багатьох організацій недостатні для захисту їхньої хмарної інфраструктури.

Цьому сприяє кілька факторів. Хмарна інфраструктура розроблена таким чином, щоб її можна було легко використовувати та надавати можливість легкого обміну даними, що ускладнює організаціям забезпечення доступу до даних лише авторизованим сторонам. Крім того, організації, які використовують хмарну інфраструктуру, також не мають повної видимості та контролю над своєю інфраструктурою, а це означає, що вони повинні покладатися на елементи керування безпекою, які надає їхній постачальник хмарних послуг (CSP), щоб налаштувати та захистити свої хмарні розгортання. Оскільки багато організацій не знайомі з захистом хмарної інфраструктури та часто мають багатохмарні розгортання – кожне з різним набором засобів безпеки, наданих постачальником, неправильна конфігурація або недогляд у безпеці можуть легко залишити хмарні ресурси організації відкритими для зловмисників.

На відміну від локальної інфраструктури організації, їх хмарні розгортання знаходяться поза периметром мережі та доступні безпосередньо з загальнодоступного Інтернету. Хоча це є активом для доступності цієї інфраструктури для співробітників і клієнтів, це також полегшує зловмиснику отримання неавторизованого доступу до хмарних ресурсів організації. Неправильно налаштований захист або скомпрометовані облікові дані можуть дозволити зловмиснику отримати прямий доступ, можливо, без відома організації.

CSP часто надають своїм клієнтам низку інтерфейсів прикладного програмування (API) та інтерфейсів. Загалом, ці інтерфейси добре задокументовані, щоб зробити їх зручними для використання клієнтами CSP.

Однак це створює потенційні проблеми, якщо клієнт належним чином не захистив інтерфейси своєї хмарної інфраструктури. Документація, розроблена для замовника, також може бути використана кіберзлочинцем для виявлення та використання потенційних методів доступу та викрадання конфіденційних даних із хмарного середовища організації.

Багато людей мають надзвичайно слабкий захист паролів, включаючи повторне використання паролів і використання слабких паролів. Ця проблема посилює вплив фішингових атак і витоку даних, оскільки дає змогу використовувати один викрадений пароль для кількох різних облікових записів.

Викрадення облікових записів є однією з найсерйозніших проблем безпеки в хмарі, оскільки організації все більше покладаються на хмарну інфраструктуру та програми для основних бізнес-функцій. Зловмисник, маючи облікові дані співробітника, може отримати доступ до конфіденційних даних або функцій, а скомпрометовані облікові дані клієнта дають повний контроль над їхнім обліковим записом в Інтернеті. Крім того, у хмарі організаціям часто не вистачає можливості ідентифікувати ці загрози та реагувати на них так само ефективно, як у локальній інфраструктурі.

Хмарні ресурси організації розташовані за межами корпоративної мережі та працюють на інфраструктурі, якою компанія не володіє. Як наслідок, багато традиційних інструментів для

досягнення видимості мережі неефективні для хмарних середовищ, а деяким організаціям бракує інструментів безпеки, орієнтованих на хмару. Це може обмежити можливості організації контролювати свої хмарні ресурси та захищати їх від атак.

Хмара створена для полегшення обміну даними. Багато хмар надають можливість явно запросити співавтора електронною поштою або надіслати посилання, яке дає змогу будь-кому, хто має URL-адресу, отримати доступ до спільного ресурсу.

Хоча цей простий обмін даними є перевагою, він також може бути серйозною проблемою безпеки хмари. Використання спільного доступу на основі посилань – популярного варіанту, оскільки це простіше, ніж явно запросити кожного співавтора – ускладнює контроль доступу до спільного ресурсу. Спільне посилання може бути перенаправлено комусь іншому, викрадене під час кібератаки або здогадане кіберзлочинцем, забезпечуючи несанкціонований доступ до спільного ресурсу. Крім того, обмін на основі посилань унеможливлює скасування доступу лише до одного одержувача спільного посилання.

Внутрішні загрози є серйозною проблемою безпеки для будь-якої організації. Зловмисник уже має авторизований доступ до мережі організації та деяких конфіденційних ресурсів, які вона містить. Спроби отримати такий рівень доступу – це те, що відкриває більшість зловмисників до їхньої цілі, що ускладнює для непідготовленої організації виявлення зловмисного інсайдера.

У хмарі виявити зловмисника ще складніше. Завдяки хмарному розгортанню компаніям не вистачає контролю над базовою інфраструктурою, що робить багато традиційних рішень безпеки менш ефективними. Це, а також той факт, що хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету та часто страждає від неправильних конфігурацій безпеки, ще більше ускладнює виявлення зловмисників.

Кіберзлочинність – це бізнес, і кіберзлочинці обирають свої цілі на основі очікуваної прибутковості своїх атак. Хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету, часто неналежним чином захищена та містить велику кількість конфіденційних і цінних даних. Крім того, хмара використовується багатьма різними компаніями, а це означає, що успішна атака може бути повторена багато разів з високою ймовірністю успіху. Як наслідок, хмарні розгортання організацій є звичайним об’єктом кібератак.

Хмара необхідна для ведення бізнесу багатьма організаціями. Вони використовують хмару для зберігання важливих бізнес-даних і запуску важливих внутрішніх і клієнтських програм.

Це означає, що успішна атака типу «відмова в обслуговуванні» (DoS) проти хмарної інфраструктури, швидше за все, матиме серйозний вплив на низку різних компаній. У результаті DoS-атаки, коли зловмисник вимагає викуп, щоб зупинити атаку, становлять значну загрозу для хмарних ресурсів організації.

Література

1. Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
2. Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl 75:200–222
3. Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
4. Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88
6. Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res Comput Commun Eng 2(10):6245–6253
7. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11