УДК 004.056
DOI: 10.31673/2409-7292.2021.042935

Осьмак Д.П., Дмітрієв В.Є., Свертока В.В.

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ДОСТУПУ ДО ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ MICROSOFT CLOUD APP SECURITY

Досліджено методи та засоби забезпечення доступу до хмарних сервісів на прикладі рішення Microsoft Cloud App Security. Визначено призначення, основні функції та принципи роботи рішення Microsoft Cloud App Security. На основі досліджень проведених в роботі розроблено варіант технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи та рекомендації щодо застосування даної технології на підприємстві.

Ключові слова: корпоративна інформаційна система, кібербезпека, захист доступу, хмарний сервіс, методи та засоби casb, технологія захищеного доступу.

Вступ

Перехід в хмару збільшує гнучкість як для співробітників, так і для IT-відділу. Однак це також створює нові проблеми і складнощі для забезпечення безпеки корпоративної інформаційної системи. Щоб отримати всі переваги хмарних додатків і послуг, IT-команда повинна знайти правильний баланс підтримки доступу при збереженні контролю для захисту критично важливих даних.

Microsoft Cloud App Security - це брокер безпеки хмарного доступу (CASB), який підтримує різні режими розгортання, включаючи збір журналів, з'єднувачі API і зворотний проксі. Він забезпечує широку видимість, контроль над переміщенням даних і складну аналітику для виявлення і боротьби з кіберзагрозами у всіх хмарних сервісах різних виробників [1].

Вищенаведені аргументи актуалізують дослідження щодо забезпечення кібербезпеки корпоративної інформаційної системи при використанні доступу до хмарних сервісів Microsoft Cloud App Security.

Кібербезпека використання хмарних сервісів

Більшість співробітників компаній все частіше використовують публічні хмарні сервіси для виконання своїх робочих завдань, але це відбувається без участі ІБ-департаментів і, відповідно, без проведення оцінки ризику використання цих сервісів, а також без урахування можливого їх впливу на дотримання внутрішніх політик ІБ і відповідності вимогам зовнішніх регуляторів. Така модель використання хмарних сервісів приводить до відповідних ризиків, що вимагає від ІБ департаментів знайти баланс між зручністю використання хмарних сервісів та забезпеченням кібербезпеки. Отже, незважаючи на цілий ряд переваг використання хмарних сервісів і перенесення даних в хмари створює для компаній проблему щодо забезпечення кібербезпеки в питанні керування великою кількістю пристроїв, які використовують співробітника для доступу в хмарні сервіси. [2].

До основних проблем кібербезпеки хмари можна віднести наступне (рис. 1):

відсутність видимості контролю;

тіньові IT;

ймовірність випадкової публікації даних;

навмисний виток даних;

спотворення або втрата критичних даних;

невідповідність вимогам регуляторів;

присутність хмарних шкідливих програм;

ймовірність розповсюдження шкідливого ПЗ на всю мережу.

На ринку все ще залишаються організації, які виключають ризики, які пов'язані з хмарними додатками / сервісами, і роблять це шляхом повного блокування їх використання. Але цей підхід не є ефективний і може мати негативний вплив використовувані бізнес-процеси сучасних організацій, наприклад, там, де співробітники компанії вже мали досвід

використання в своїй роботі хмарних сервісів. Оскільки вже зараз, з економічною обстановкою в країні і світі більшість компаній все ж переводять свої робочі процеси в хмару і все частіше впроваджують до використання хмарні сервіси, виникає питання: які ж заходи забезпечення безпеки необхідно зробити, щоб безпечно користуватися хмарними сервісами і не боятися переносити корпоративні дані в хмари? Для вирішення питань щодо забезпечення кібербезпеки в хмарах і дотримання вимог внутрішніх служб інформаційної безпеки та зовнішніх регулюючих органів в частині роботи з хмарними даними на ринку пропонуються рішення класу Cloud Access Security Brokers (CASB) - брокер безпеки хмарного доступу [3].

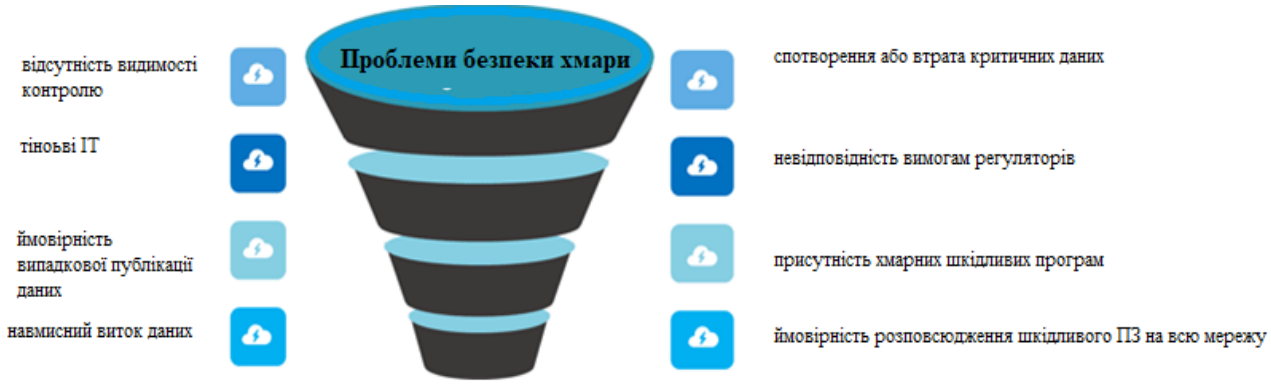

Рис 1. Проблеми безпеки хмари

Мета роботи – розробити варіант забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи та рекомендації щодо застосування технології на підприємстві.

Архітектура Microsoft Cloud App Security

Системи CASB на початку свого розвитку були в основному зосереджені на контролі доступу до бек-офісних додатків, що поставляються як Software as a Service (SaaS), таким як CRM, ERP, HR, спільне використання файлів (EFSS), хмарні додатки типу G Suite і Microsoft Office 365 і служби технічної підтримки (Service desk). Зараз же область їх застосування включає в себе інструменти для контролю доступу до більш широкого спектру хмарних сервісів: Platform as a Service (PaaS) і Infrastructure as a Service (IaaS).

Хмарні сервіси системи CASB допомагають організаціям контролювати хмарні додатки і сервіси, як офіційно дозволені політиками ІБ компаній до використання, так і не дозволених, які вважаються неправомірними. CASB надає видимість, необхідну для забезпечення безпеки хмарних додатків, і можливість швидко і ефективно реагувати на зовнішні та внутрішні загрози. Провідні аналітичні агентства до цього класу рішень відносять такі основні функціональні блоки: наочність, захист даних, захист від загроз і відповідність вимогам регулюючих органів [4].

Розглянемо архітектуру Cloud App Security, яка надасть основне уявлення щодо методів та засобів роботи в хмарному середовищі компанії (рис. 2). Cloud App Security дозволяє отримувати інформацію про хмарі за рахунок використання наступних засобів:

Cloud Discovery використовується для зпівставлення і визначення хмарного середовища і хмарних додатків, які використовує компанія;

застосовує і скасовує санкціонування додатків в хмарі;

використовує *прості* в розгортанні з'єднувачі додатків, які застосовують переваги інтерфейсів API постачальників, для моніторингу і контролю додатків, до підключаються працівники компанії.

використовує *захист* на основі Управління умовним доступом до додатків, забезпечуючи можливість відстеження і контролю доступу та дій, які виконуються в ваших хмарних додатках;

забезпечує *безперервний контроль* завдяки установці політик і їх постійного налаштування.

Дана архітектура забезпечує забезпечує роботу платформи Cloud App Security основним призначенням якої є [1]:

виявлення та адміністрування використання тіньових IT. Визначає хмарні додатки, IaaS і служби PaaS, які використовує компанія. Аналізувати шаблони використання, а також оцінка рівня ризику і готовності бізнес-процесві використовувати більш ніж 16 000 додатків SaaS, запобігаючи виникненню більш ніж 80 типів ризиків. Це дозволить забезпечити безпеку і відповідністьі вимогам щодо управління бізнес-процесів компанії.

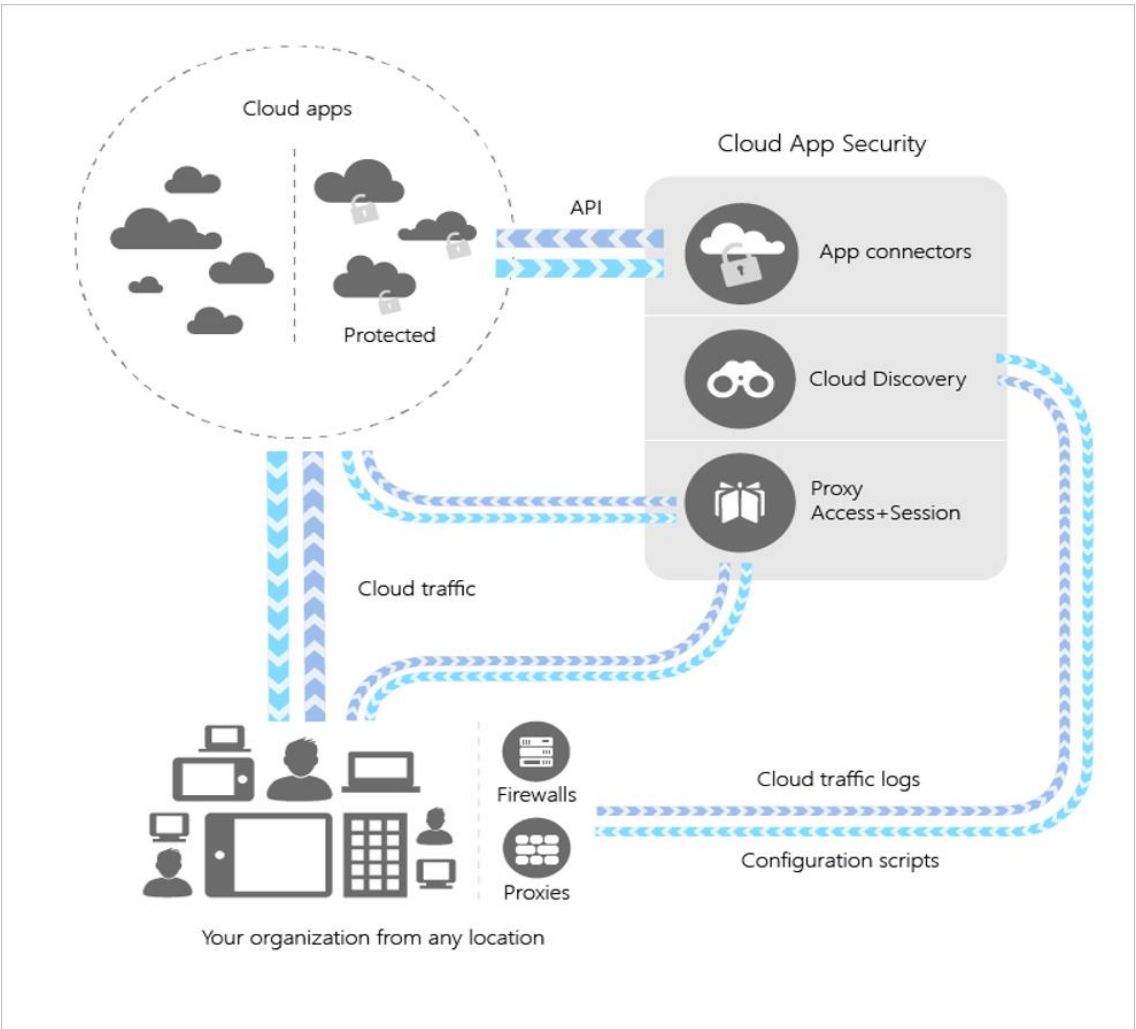

Рис. 2. Архітектура Microsoft Cloud App Security

захист конфіденційних даних в будь-якому місці в хмарі. Надає можливість аналізувати, класифікувати і захищати конфіденційні відомості від розкриття при зберіганні. При використанні готових політик і автоматизовані процеси допоможе при застосування засобів управління в реальному часі до всіх хмарних додатків.

захист від кіберзагроз та аномалій. Визначається незвичайна поведінка хмарних додатків для ідентифікації програм-шантажистів, скомпрометованих користувачів або шахрайських програм, аналізує шаблони використання з високим ризиком, а також автоматично застосовує виправлення, щоб запобігти ризикам для компанії.

оцінка відповідності хмарних додатків. Оцінка, чи відповідають хмарні додатки відповідним вимогам, включаючи відповідність нормативним вимогам і галузевим стандартам. Дозволяє запобігти витоку даних для невідповідних додатків і обмежує доступ до контрольованих даних.

Для розгортання Microsoft Cloud App Security у компанії повинна бути ліцензія на використання Cloud App Security. Microsoft Cloud App Security - це служба підписки на основі користувачів. Кожна ліцензія розрахована на кожного користувача на місяць. Microsoft Cloud App Security можна ліцензувати як окремий продукт або як частину декількох різних планів ліцензування. Коли ми говоримо про «повну пропозицію CASB», мається наувазі що це пропозиція, яка включає всі можливості Cloud App Security, Office 365 Cloud App Security і Cloud App Discovery.

Технологія виявлення і контролю тіньових IT у мережі

За допомогою Cloud Discovery є можливість виявити використовувані додатки, визначити їх ризик, налаштувати політики для визначення нових ризикованих додатків і зробити ці програми несанкціонованими, щоб вони спочатку блокувалися проксі-сервером або брандмауером [5].

Виявлення і визначення тіньових IT

Оцінка та аналіз

Управління додатками

Розширені звіти про виявлення тіньових IT

Контроль санкціонованих додатків

Розглянемо технологію як виявляти і контролювати тіньові IT у мережі компанії.

Етап 1. Виявлення і визначення тіньових IT

1. *Виявлення тіньових IT*. Використовується Cloud Discovery для оцінки системи безпеки своєї організації - це допомагає дізнатися, що насправді відбувається в мережі. Це можна зробити за допомогою будь-якого з наступних методів:

Щоб швидко почати роботу з Cloud Discovery, використовуйте інтеграцію з ATP в Microsoft Defender. Початкова підтримка інтеграції дозволяє відразу ж почати збір даних хмарного трафіку на пристроях під управлінням Windows 10 всередині і поза вашої мережі.

Щоб охопити всі підключені до мережі пристрої, важливо розгорнути збір журналів даних Cloud App Security на брандмауерах та інших проксі-серверах, який буде збирати дані з кінцевих точок і відправляти їх в Cloud App Security для аналізу.

Інтеграція Cloud App Security з проксі-сервером. Cloud App Security спочатку підтримує інтеграцію з рядом сторонніх проксі-серверів, включаючи Zscaler.

Так як в різних групах користувачів, регіонах і бізнес-групах використовуються різні політики, можливо, є сенс створити для них окремі звіти про тіньові IT. Запустивши Cloud Discovery в своїй мережі, ознайомтеся з створюваними безперервними звітами і панеллю моніторингу Cloud Discovery, щоб отримати повне уявлення про використовувані у вашій організації додатках. Рекомендується переглядати їх за категоріями, так як часто несанкціоновані програми застосовуються в робочих цілях, якщо потрібна функція в санкціонованих відсутня.

2. *Визначення рівнів ризику додатків*. Каталог хмарних додатків Cloud App Security дозволяє детально аналізувати ризики, пов'язані з кожним виявленим додатком. Каталог ризиків Cloud App Security включає більше 16 000 додатків, які оцінюються більш ніж по 80-ти факторам ризику. Фактори ризику включають як загальну інформацію про програму (в яких регіонах вона використовується, хто його видавець), так і засоби безпеки (підтримка шифрування неактивних даних, журнал аудиту призначених для користувача дій).

На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені* додатки. Відфільтруйте список виявлених додатків в організації, про що цікавлять вас факторам ризику. Наприклад, ви можете використовувати розширені фільтри, щоб знайти всі додатки з оцінкою ризику нижче 8.

Щоб отримати докладні відомості про фактори ризику безпеки програми, клацніть його ім'я і перейдіть на вкладку *Відомості*.

Етап 2. Оцінка і аналіз.

1. *Оцінка відповідності.* Перевірте, чи сертифіковані додатки які відповідні стандартам вашої організації, таким як HIPAA, SOC2 і GDPR.

На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені додатки*. Відфільтруйте список виявлених додатків в організації, які цікавлять вас за фактором ризику відповідності. Наприклад, використовуйте запропонований запит, щоб відфільтрувати додатки, які не відповідають вимогам.

Щоб отримати докладні відомості про фактори ризику відповідності додатки, клацніть його ім'я і перейдіть на вкладку *Відомості.* Дочекайтеся отримання повідомлення, якщо виявлений додаток пов'язаний з нещодавно опублікованими порушенням безпеки, виявлено порушення безпеки програми необхідно виявити всіх користувачів, IP-адреси і пристрої, які зверталися до уразливого додатка за останні 90 днів, і застосуєте відповідні засоби контролю.

2. *Аналіз використання*. Тепер, коли виявлено, чи варто використовувати додаток в організації, дізнайтеся, хто і як його використовує. Якщо воно використовується тільки в обмеженому ряді випадків, можливо, це нормально. Однак якщо воно застосовується все частіше, то ви напевно захочете знати про це, щоб прийняти рішення про можливе блокування. Для цього:

На порталі Cloud App Security в розділі *Виявлення* клацніть *Виявлені додатки* і виберіть конкретний додаток для аналізу. На вкладці *Використання* показано, скільки активних користувачів працюють з додатком і скільки трафіку воно створює. З цього ви вже зможете в цілому зрозуміти, що відбувається з додатком. Потім, якщо ви захочете дізнатися, хто конкретно використовує додаток, ви можете розкрити більш докладні відомості, клацнувши *Всіх активних користувачів.* Це важлива дія дасть вам актуальну інформацію: наприклад, якщо ви виявите, що всі користувачі певної програми - з відділу маркетингу, то можливо, такий додаток необхідно організації. Якщо воно пов'язане з високим ризиком, слід запропонувати альтернативу, перш ніж блокувати його [6].

Дізнайтеся докладніше про використання виявлених додатків. Переглядайте піддомени і ресурси, щоб дізнатися про конкретні дії, доступі до даних і використанні ресурсів в хмарних службах.

3. Виявлення альтернативних додатків: знайдіть в каталозі хмарних додатків більш безпечні програми, які забезпечують такий же бізнес-функціонал, як у виявлених додатків з ризиком, але на відміну від них відповідають політиці вашої організації. Розширені фільтри дозволять шукати додатки тієї ж категорії, які відповідають різним використовуваним вами параметрам контролю безпеки.

Етап 3. Управління додатками

Управління хмарними додатками. Cloud App Security допомагає контролювати використання додатків у вашій організації. Визначивши в ній типові дії і шаблони поведінки, ви можете створювати власні теги для класифікації додатків відповідно до їх бізнес-статусом і обгрунтуванням використання. Ці теги потім можна застосовувати для конкретних цілей моніторингу, наприклад для виявлення великих обсягів вхідного трафіку в додатках, позначених тегом хмарного сховища з високим ризиком. Тегами додатків можна управляти в розділі *Параметри Cloud Discovery> Теги додатків.* Надалі ви можете використовувати ці теги для фільтрації на сторінках Cloud Discovery і створювати з їх допомогою політики.

Рекомендується управляти виявленими додатками за допомогою колекції Azure Active Directory (Azure AD): У Cloud App Security також використовується власна інтеграція з Azure Active Directory, яка дозволяє управляти виявленими додатками в колекції Azure Active Directory. Для додатків, які вже відображаються в колекції Azure Active Directory, можна використовувати єдиний вхід і управляти ними за допомогою Azure Active Directory. Для

цього знайдіть рядок потрібної програми, клацніть три точки в кінці рядка і виберіть Керувати додатком в Azure Active Directory.

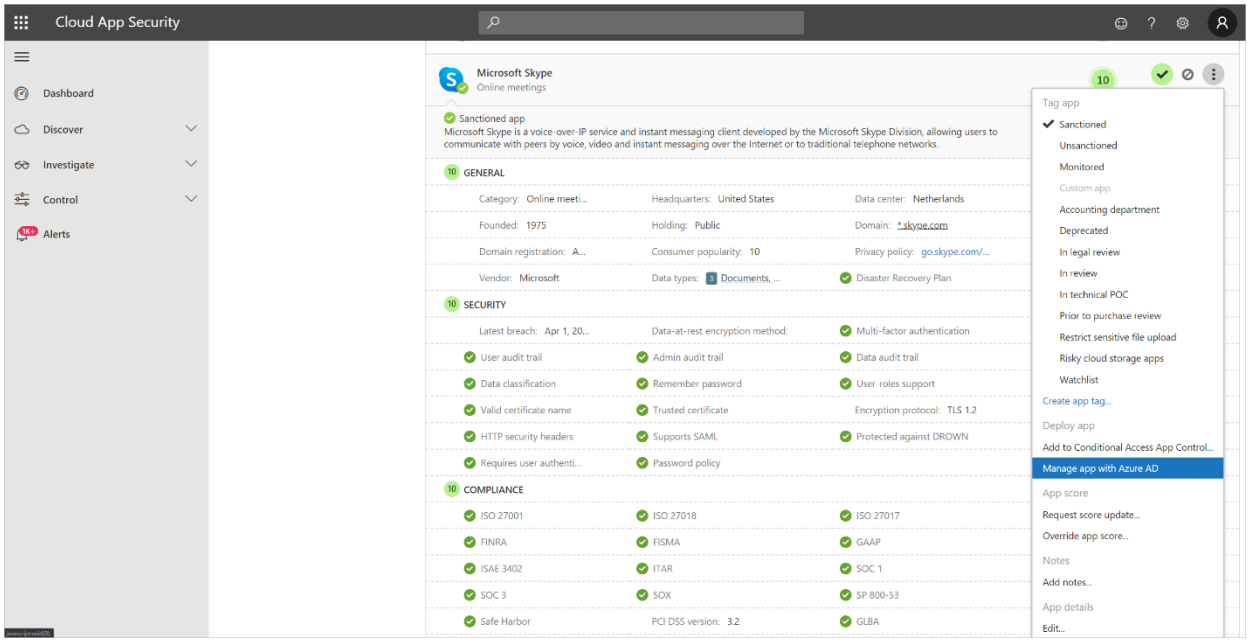

Рис. 3. Вікно керування додатками

Безперервний моніторинг. Провівши детальний аналіз додатків, можливо, необхідно створити політики їх моніторингу та необхідні елементи управління.

Тепер прийшов час створити політики, щоб отримувати автоматичні оповіщення про важливі для вас події. Наприклад, ви можете створити політику виявлення додатків, яка буде повідомляти про різке збільшення обсягів скачування або трафіку в сюжеті вашого додатку. Для цього слід включити політики *Незвичайна поведінка* у виявлених користувачів, Перевірка додатків хмарного сховища на відповідність і *Нов ризикований додаток*. Слід також налаштувати політику для повідомлень по електронній пошті або текстовими повідомленнями.

Відкрийте сторінку попереджень і використовуйте фільтр *Тип політики*, щоб знайти попередження виявлення додатків. При виявленні будь-то додатків, відповідних політикам, рекомендуємо провести додатковий аналіз, наприклад зв'язавшись з їх користувачами, щоб отримати обгрунтування їх застосування в організації. Потім повторіть дії на етапі 2, щоб оцінити ризик додатку. Після цього прийміть рішення про подальші дії: затвердите додаток для майбутнього використання або щоб позначити його як несанкціоноване, щоб доступ до нього користувачам блокувався брандмауером, проксі-сервером або захищеним веб-шлюзом.

Етап 4. Розширені звіти про виявлення тіньових IT

Крім установок звіту, доступних в Cloud App Security, є можливість інтегрувати журнали Cloud Discovery в Azure Sentinel для подальшого вивчення і аналізу. Після переміщення даних в Azure Sentinel, можна переглядати їх на панелях моніторингу, виконувати запити за допомогою мови запитів Kusto, експортувати запити в Microsoft Power BI, інтегрувати їх з іншими джерелами і створювати власні оповіщення.

Етап 5: Контроль санкціонованих додатків

1. Щоб увімкнути управління додатками через API, підключіть додатки за допомогою API для безперервного моніторингу.

2. Захист додатоків за допомогою *Управління умовним доступом до додатків*.

Слід пам'ятати, що хмарні додатки щодня оновлюються, і постійно виходять нові хмарні програми. Через це співробітники весь час використовують нові додатки, тому важливо відстежувати, перевіряти та оновлювати ваші політики, а також контролювати, які

програми використовують користувачі і як вони з ними працюють. Ви завжди можете відкрити панель моніторингу Cloud Discovery і дізнатися, які нові додатки зараз використовуються, а потім знову виконати етапи для забезпечення захисту вашої організації і її даних.

Висновки

В роботі досліджено технологію забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи на базі рішення Microsoft Cloud App Security. Визначено методи та засоби забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи, які реалізовані в Microsoft Cloud App Security. Встановлено основні функції та принципи роботи програмного комплексу Microsoft Cloud App Security. Визначено архітектуру Microsoft Cloud App Security для розуміння загального стану хмари в додатках SaaS і хмарних сервісах, і тому виявлення тіньових IT і управління додатками є ключовими варіантами використання. Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи.

Таким чином, правильна реалізація технології забезпечення захищеного доступу до хмарних сервісів корпоративної інформаційної системи на базі рішення Microsoft Cloud App Security має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства.

Перелік посилань

1. Інтернет ресурс. Хмарні сервіси на базі Microsoft для бізнесу [Електронний ресурс] режим доступу: https://www.lankey.ru/oblachnie-servisi/ .
2. Інтернет ресурс. CASB [режим доступу https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-security-broker].
3. CASB A Complete Guide - 5STARCooks (September 29, 2019)- 2020. – 302p.
4. Cloud Access Security Broker A) Complete Guide - 5STARCooks (September 6, 2019)– 2020. – 298p.
5. Using Oracle CASB Cloud Service., Release 20.1.1.0 [Електронний ресурс] режим доступу: https://www.lankey.ru/oblachnie-servisi - Oracle - July 2020 -727p
6. Осьмак Д.П. Технологія забезпечення захисту хмарних сервісів на базі рішення Microsoft Cloud App security [Електронний ресурс]. - Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки».- Київ, ДУТ.- с. 129-132[режим доступу:http://www.dut.edu.ua/uploads/p_1739_27992763.pdf]
7. Miller R. Who Has the Most Web Servers? [Electronic resource] / R. Miller - Access mode:http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the- most-web-servers/ - 27.09.2019.
8. Оплачко Е.С. Облачньїе технологии и их применение в задачах вьічислительной биологии [Злектронньій ресурс] / Е.С. Оплачко., Д.М. Устинин., М.Н. Устинин - Режим доступа: http://www.matbio.org/2013/Oplachko_8_449.pdf - 28.09.2019.
9. PaaS, DBaaS, SaaS... Что все ^то значит? [Злектронньій ресурс] - Режим доступа: https://habr.com/ru/company/kingservers/blog/310022/ - 28.09.2019.
10. Wadiwala R. Cloud Database - DBaaS (Database as a Service) [Electronic resource] / R. Wadiwala - Access mode: https://labs.sogeti.com/cloud- database-dbaas-database-as-a-service/ - 29.09.2019
11. Demchenko Y. Defining inter-cloud architecture for interoperability and integration [Text] / Y. Demchenko, C. Ngo, M.X. Makkes, R. Strijkers, C. de Laat // Proceeding of the 3rd International Conference on Cloud Computing, GRIDs and Virtualization, Nice, France, July 22-27, 2012 y. - pp. 174-180
12. Malik N.A. Threat modeling in pervasive computing paradigm [Text] / N.A. Malik, M.Y. Javed, U. Mahmud // Proceedings of the Mobility and Security, New Technologies, Tangier, November 5-7, 2008 y. - pp. 1-5
13. McRee R. PTA: Practical threat analysis [Text] / R. McRee // Proceedings of the Information Systems Security Association, London, September 1516, 2008 y. - pp. 37-40
14. Jehangir A. Securing inter-cluster communication in personal networks [Text] / A. Jehangir // Proceedings of the 4th Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services, Philadelphia, August 6-10, 2007 y. - pp. 1-6
15. Bertino E. L. Security for Web Services and Service-Oriented Architectures [Text] / E. L. Bertino // Proceedings of the 2th Annual International Conference on Information Security, New York, USA., September 2-7, 2012 y. - pp. 35-69

Надійшла: 06.10.2021 Рецензент: д.т.н., професор Гайдур Г.І.