ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія захисту файлового серверу компанії на базі SecureSphere File Security»

Виконав студент 6 курсу, групи БСЗМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Хотінь Кароліна Юріївна
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MX – Сервер керування

WAF - Web application firewall

ADC - Application Defense Center

UUT - Universal User Tracking

EIK - External-in-Kernel

PCAP - Packet Capture

ВСТУП

Актуальність дослідження. Кожну хвилину… час… день… місяць… і рік на файлових серверах постійно створюються файли в організації - конфіденційні регульовані дані постійно змінюються. Imperva File Security дозволяє захищати дані файлів, сховищ і систем SharePoint, і повністю відповідають нормативним вимогам. Imperva File Security надає всі необхідні інструменти, а в комплексі технологію, яка забезпечить захист від витоку, крадіжки даних та надасть можливості швидкого реагування на інциденти.

Таким чино необхідно визначити методи та засоби захисту файлових серверів в інфраструктурі організації. Застосування комплексних методів та засобів дозволять захистити файлові сервера організації на основі обраного рішення. Вищенаведені аргументи актуалізують дослідження захисту файлових серверів в організації.

Об'єкт дослідження – процес забезпечення безпеки файлових серверів організації.

Предмет дослідження – технологія захисту файлових серверів в інфраструктурі організації.

Мета роботи – розробити варіанти захисту файлового серверу в інфраструктурі організації та рекомендації щодо застосування технології.

Наукові завдання:

Провести аналіз щодо ролі і місця файлових серверів в інфраструктурі організації;

визначити основні загрози серверній інфраструктурі організації та провести порівняння рішень щодо захисту файлових серверів організації;

проаналізувати методи та засоби захисту файлових серверів організації;

розробити варіант технології захисту файлового серверу на базі рішення SecureSphere File Security та розробити рекомендації фахівцям з кібербезпеки щодо застосування обраної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту привілейованих даних користувачів інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці варіанту комплексного захисту файлового серверу на базі рішення SECURESPHERE FILE SECURITY що дозволить ефективно функціонувати системі організації для виконання всіх бізнес-процесів.

Апробація результатів. Результати дослідження доповідались на всеукраїнській конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ НЕОБХІДНОСТІ ЗАХИСТУ ФАЙЛОВИХ СЕРВЕРІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Роль і місце серверів в інформаційній системі організації

При необхідності зберігання великих масивів даних та організації віддаленого доступу користувачів до них необхідно використовувати файловий сервер. Його роль в IT-інфраструктурі підприємства полягає у наданні користувачам певного місця для робочих файлів, з подальшим відкриттям та редагуванням залежно від ієрархії прав. Фактично пристрій визначає, які папки можуть редагуватися та переглядатися конкретним співробітником компанії[1].

Доцільність встановлення файлового сервера.

Крім можливості централізованого управління та розподілу прав доступу, файлове обладнання спрощує процес виконання колективної роботи з базами даних та документацією. Це виявляється у виключенні відкриття кількох версій одного документа при одночасній зміни користувачів та усунення ресурсних обмежень[1].

Установка файлового сервера має низку додаткових переваг, серед яких[1]:

простота знаходження необхідної інформації;

високий рівень безпеки та захисту даних на відміну від фізичного комп'ютера;

можливість розвантажити пристрої користувача;

зручна робота з великими масивами даних;

гарантія безпеки інформації навіть при виході обладнання з ладу.

Щоб запобігти ймовірності виникнення програмних та технічних помилок, налаштування файлового сервера варто довірити фахівцеві. Сама процедура передбачає вибір комплектуючих, організацію процесу віддаленого доступу та встановлення ПЗ [1].

При виборі файлового сервера необхідно визначати критерії, які потребують уваги.

Під час встановлення обладнання слід перевірити сумісність мережевих пристроїв та операційної системи. Таку роль виконують операційні системи Windows, Linux або MacO та інші сучасні версії.

Для вибору файлового серверу необхідно брати до уваги наступні фактори:

відмовостійкість - від рівня залежить здатність збереження даних після виходу пристрою з ладу;

доступний обсяг пам'яті та можливість його розширення;

швидкість доступу до інформації, що відображає час відкриття та копіювання файлів.

Залежно від особливостей організації, роль файлового сервера може виконувати і звичайний комп'ютер. При великій кількості користувачів перевагу краще надати виділеному серверу з встановленим програмним забезпеченням або без нього [1].

Повноцінна комунікація підприємства із зовнішнім світом забезпечується розвиненою технічною інфраструктурою: електронна пошта, база даних, 1С, корпоративний сайт, система клієнт-банк, файлове сховище та ін. Коректна робота всіх систем підприємства забезпечується за рахунок грамотного настроювання серверів.

Розглянемо основні задачі при створенні та встановленні сервера.

Створення сервера – комплекс заходів щодо створення місця зберігання систем та програм, а також їх баз даних. Серверна структура виконує важливу роль, тому що вона забезпечує місце для встановлення систем та додатків, пов'язаних з ними баз даних та надає доступ користувачів до них для підвищення їх взаємодії. Встановлення та налаштування серверів – є необхідною опцією для більшості підприємств [3].

Для створення та реалізації необхідних функцій серверу необхідно на початковому етапі провести аналіз вводних. Для ефективного підбору та створення сервера важливо визначити стек завдань та технологій, які необхідні. Для цього підбирається обладнання з необхідними параметрами:

Перелік завдань.

Додаткові функції.

Об'єм сховища.

Тип процесора: GPU, CPU.

Мінімальний обсяг оперативної пам'яті (RAM).

Наявність віддаленого модуля доступу.

Тип установки (вид корпусу).

Кількість жорстких дисків та їх тип.

Операційна система.

Блок живлення.

Усі ці параметри необхідні формалізації технічного рішення.

Для встановлення та налаштування серверу мати на увазі збір, тестування та налаштування всіх елементів:

Вибір та купівля комплектуючих або сервера в зборі.

Складання сервера та проведення його тестування.

Встановлення та налаштування операційної системи.

Встановлення та налаштування спеціалізованого програмного забезпечення під завдання підприємства (1С, поштовий клієнт, інтернет-банкінг, бази даних та інше).

Налаштування резервного копіювання.

Налаштування та аудит політик безпеки.

Тестування навантаження.

Введення в експлуатацію [3].

Корпоративні серверні комплекси монтуються у спеціальні стійки чи серверні шафи. Обладнання вибирається з урахуванням конструктивних особливостей приміщення. Важливо, щоб обрана територія мала надійну вентиляцію та охолодження, а також давала вільний доступ до стійок. Також необхідно продумати розташування резервного електроживлення та умови пожежної безпеки. Монтаж обладнання складається з кількох етапів:

Встановлення стійок.

Підключення електричного та мережевого кабелю.

Установка шасі під обладнання та фіксація комплектуючих на шасі.

Тестовий запуск системи перевірки працездатності.

Після встановлення всіх елементів відбувається процедура налаштування.

Після визначення завдань та підбору оптимального сервера необхідно налаштувати обладнання та програмне забезпечення. Кожен сегмент має свої особливості налаштування [3].

VPN СЕРВЕР

Мобільність та оперативність – одне з головних завдань бізнесу. VPN дозволяє отримати доступ до бази даних підприємства із віддаленого офісу. Тобто створити умови для спільної роботи співробітників із різних офісів (опціонально). З налаштуванням VPN підвищується безпека мережі [3].

DNS СЕРВЕР

Підключення DNS – технічна необхідність подальшої реалізації функціоналу ПЗ. Наприклад, щоб використовувати Active Directory або підключити поштовий сервіс. Послуга йде в базовому наборі опцій, полегшує взаємодію з мережею та дозволяє підключити ряд функцій [3].

НАЛАШТУВАННЯ СЕРВЕРУ LINUX

Для підприємств, які працюють на базі операційної системи LINUX, актуальним питанням стає налагодження та запуск сервера Linux [3]. При налаштуванні проводиться запуск усіх ключових елементів:

Файлообмінник.

Веб-сервер.

СУБД.

Firewall (Брандмауер).

Балансування запитів.

На даний момент подібні ОС показують найвищу безпеку.

БАЗИ ДАНИХ SQL

Сервер баз даних прискорює роботу та оптимізує процеси. Він необхідний підприємств, де використовують 1С:Бухгалтерію. Вартість налаштування сервера 1С залежить від конфігурації та типу системи [3].

ТЕРМІНАЛЬНИЙ СЕРВЕР WINDOWS

Сервера терміналів знижують фінансові витрати на дозволи та ліцензування. Найбільш відомий приклад експлуатації у роботі термінального сервера – 1С.

При встановленні важливо враховувати, що сховище має бути розділене на 2 частини: малу – під операційну систему та велику, яка виконуватиме роль сховища даних.

Підключення термінального сервера дозволяє працювати з 1С так, ніби програмне забезпечення завантажене безпосередньо на ПК, це суттєво спрощує роботу, тому що немає необхідності постійно навантажувати базу під час експлуатації. Крім того, реалізація задачі відкриває можливість працювати разом із філіями та іншими підрозділами підприємства, які фізично знаходяться в іншому місті, країні [3].

WEB СЕРВЕР

Головним інструментом комунікацій та інформування для більшості став інтернет. Тому навіть невеликі компанії створюють свій сайт. Не важливо, чи це повноцінний корпоративний портал або односторінй з презентацією послуг, для його роботи потрібен хостинг і домен. Щоб знизити ризики втрати інформації або даних, важливо вибрати надійний та функціональний хост. Тому багато підприємств

вважають за краще хостити ресурс на своєму власному веб-сервері. Це дає абсолютний контроль за сайтом.

Встановлення веб-сервера залежить від операційної системи. Оптимальним рішенням є Linux + NGinx, для систем Windows краще використовувати IIS [3].

ПОШТОВИЙ СЕРВЕР

Доменна пошта, на відміну від безкоштовних поштових платформ, дає більш гнучкі можливості налаштування та високу безпеку. Встановлення та налаштування поштового сервера дозволить вирішити декілька ключових завдань:

Повний контроль над сервісом.

Єдиний корпоративний домен.

Можливість створення корпоративних e-mail адрес для співробітників.

Індивідуальний сервер дозволить настроїти інтелектуальний спам-фільтр та антивірусний протокол для захисту даних. Особливо актуально для підприємств із великим потоком конфіденційної інформації [3].

FTP

Для обміну даними використовується файл-сервер. З його допомогою відбувається локальний обмін файлами. Його налаштування забезпечує контроль над трансфером інформації, її розподілом. Є можливість зробити розгалуження – хто та яку інформацію може отримати для використання [3].

ACTIVE DIRECTORY

Active Directory – зручний інструмент для роботи будь-якого розміру: впровадження нових опцій, автоматизація процесів, гнучка авторизація, розподіл прав доступу [3].

1.2. Аналіз призначення файлового сервера в інформаційній системі організації

Файловий сервер

Файловий сервер – це, як правило, центральний сервер у комп'ютерній мережі, який забезпечує підключення користувачів до мережевої системи зберігання даних (СЗД).

Цей термін може означати як устаткування, і програмне забезпечення, необхідне виконання функцій файлового сервера.

Користувачі, отримавши необхідні права доступу до певних файлів в мережевий СЗД, можуть їх відкривати і редагувати, і навіть видаляти файли і папки так само, як і вони працювали на власному комп'ютері.

На файловому сервері кожному авторизованому користувачеві надається певний простір для зберігання робочих файлів (рис.1.1). Інші користувачі можуть також їх відкривати, читати та редагувати відповідно до їхніх прав доступу. Ці права встановлюються адміністратором файлового сервера. Він визначає, хто які файли та в яких папках може відкривати та переглядати, а також (якщо це дозволено) редагувати, видаляти чи додавати нові файли.

В загальному випадку архітектура інформаційної системи та місце файлового серверу показано на рис.1.1.

Рис.1.1. Місце файлового серверу в інформаційній системі організації [1]

Крім того, файловий сервер може мати підключення до інтернету, і, при відповідній конфігурації прав доступу, користувачі можуть отримувати доступ до інтернет-ресурсів, якщо доступ до них дозволений мережевим адміністратором. У деяких організаціях може адміністративно встановлюватися заборона доступу до певних ресурсів за тими чи іншим критеріям. Наприклад, може бути закритий доступ до відеохостингу Youtube, сайтам з розважальним контентом тощо. Крім того, підключення файлового сервера до інтернету забезпечує віддалений доступ користувачів до своїх папок на файловому сервері, якщо вони знаходяться не на робочому місці.

Для файлового сервера, як це було сказано раніше можуть підійти будь-які сучасні операційні системи Windows, Linux або MacOS, хоча треба мати на увазі, що мережні пристрої повинні бути з ними сумісні.

Також необхідно розуміти, що файлові сервери часто використовуються не тільки для зберігання та обробки файлів, але також як репозиторій для програм, які доступні користувачам корпоративної мережі, а також як сервер резервування.

Для забезпечення надійної роботи файлового сервера необхідно вибрати відповідне обладнання. Це перш за все процесор достатньої потужності для обслуговування заданої кількості користувачів, а також дискові накопичувачі, які мають ємність, достатню для розміщення необхідних програм та операційної системи та іншого програмного забезпечення для обслуговування користувачів організації. Важливе значення для швидкодії системи має обсяг оперативної пам'яті (ОЗП), де розміщуються модулі запущених до роботи програм. Якщо обсяг ОЗУ буде недостатній, то робота системи сильно сповільниться, і не допоможе навіть найпотужніший і найшвидший процесор.

Визначальним чинником вибору параметрів файлового сервера є кількість користувачів корпоративної мережі. Для зв'язку користувачів з файловим сервером використовуються спеціальні протоколи, наприклад протокол SMB (Server Message

Block) розроблений IBM. Він може використовуватися в локальних мережах як на пристрої Windows, так і macOS. Як протокол мережної операційної системи часто використовується NFS (Network File System). Якщо файловий сервер працює під ОС Unix, то щоб поєднати обидва типи протоколів в одній мережі як клієнти, так і файлові сервери, повинні бути оснащені програмами, які дозволяють виконувати протокол SMB в цих системах.

Для отримання віддаленого доступу до файлового сервера зазвичай використовується традиційний протокол File Transfer Protocol (FTP) або його захищений варіант SFTP (Secure FTP). Крім того, може використовуватися протокол безпечного копіювання SCP (Secure Copy) та WebDAV (Web Distributed Authoring and Versioning) – набір розширень та додатків до протоколу HTTP. WebDAV дозволяє змінювати властивості об'єктів, що зберігаються на сервері, шукати файл за властивостями, блокувати файл для редагування одним користувачем, керувати версіями файлів, а також керувати доступом до файлів на основі списків.

Переваги використання файлового сервера

Для багатьох компаній вирішальним критерієм під час використання файлового сервера для інформаційної системи організації є можливість централізованого управління та розмежування прав доступу між користувачами різних підрозділів. Крім того, легко можна забезпечити можливість колективної роботи над документами, виключивши проблему використання різних версій одного документа різними користувачами.

Інша перевага файлового сервера – це усунення ресурсних обмежень для користувачів. За винятком особистих файлів, всі робочі документи та їх резервні копії можуть бути розміщені на загальному сервері. При правильній організації структури папок та директорій користувачі отримують однакове подання всіх доступних документів в організації відповідно до своїх прав доступу.

Якщо файловий сервер налаштований для роботи через інтернет, то файли також доступні для віддаленої роботи, як і при роботі в локальній мережі. Але, на відміну від хмарного рішення, компанія продовжує зберігати контроль за файлами та їх безпекою. Це очевидна перевага перед сторонніми рішеннями щодо зберігання корпоративної інформації.

Тож основні переваги файлового сервера:

Легка організація та інвентаризація корпоративних ресурсів.

Прозорість та легкість знаходження потрібної інформації.

Зручність колективної роботи із документами.

Відсутність конфліктів версійності.

Відсутність ресурсних обмежень персональних машин користувачів.

Можливість віддаленого доступу до файлів та роботи на виїзді.

Високий ступінь захисту та безпеки даних.

Проблеми файлових серверів

Незважаючи на явні переваги, перераховані вище, визначимо проблеми файлових серверів.

Компанії часто недооцінюють обсяг роботи з встановлення, настроювання та обслуговування такого обладнання та програмного забезпечення, як файловий сервер. Іноді до цієї роботи підходять без належного планування. В результаті не тільки апаратні ресурси швидко підходять до своїх меж використання, але також і багато потенційних переваг файлового сервера не можуть виявитися повною мірою. Наприклад, за відсутності чітких принципів розподілу прав доступу користувачі часто не можуть відповідним чином виконати свої обов'язки, оскільки не можуть отримати необхідні дані. Проблеми можуть виникнути також через безладну та безсистемну побудову ієрархії папок і каталогів, якщо взагалі такої ієрархії хтось дотримується.

Ці аспекти необхідно продумати від початку, перед покупкою та встановленням файлового сервера. Також попереднього опрацювання вимагають питання захисту даних та інформаційної безпеки, особливо якщо файловий сервер призначений для

віддаленої роботи через інтернет. Встановлення та правильна конфігурація програм інформаційної безпеки така ж критична, як і навчання співробітників, які отримують доступ до сервера. Потрібне чітке розуміння персоналом того, де і як зберігати свої робочі файли на сервері, щоб унеможливити ситуації інформаційного хаосу.

1.3. Аналіз загроз для серверів інформаційної системи організації

Аналіз кількісті атак на інформаційні системи організацій збільшилася лише на 0,3% порівняно з I кварталом 2021 року. Темп зростання даного показника не змінюється так швидко, так як організації встигли адаптуватися до роботи в умовах пандемії коронавірусу. Це пов’язано з тим, що компанії вжили заходів щодо захисту мережевого периметра та налаштували системи віддаленого доступу [5].

Обсяг цілеспрямованих атак на організації зростає з кожним кварталом. У II кварталі 77% атак були цільовими [5]. Частка інцидентів, де зловмисники були націлені на приватних осіб, залишилася такою самою, як і в попередньому кварталі — 12% (рис.1.2 та 1.3).

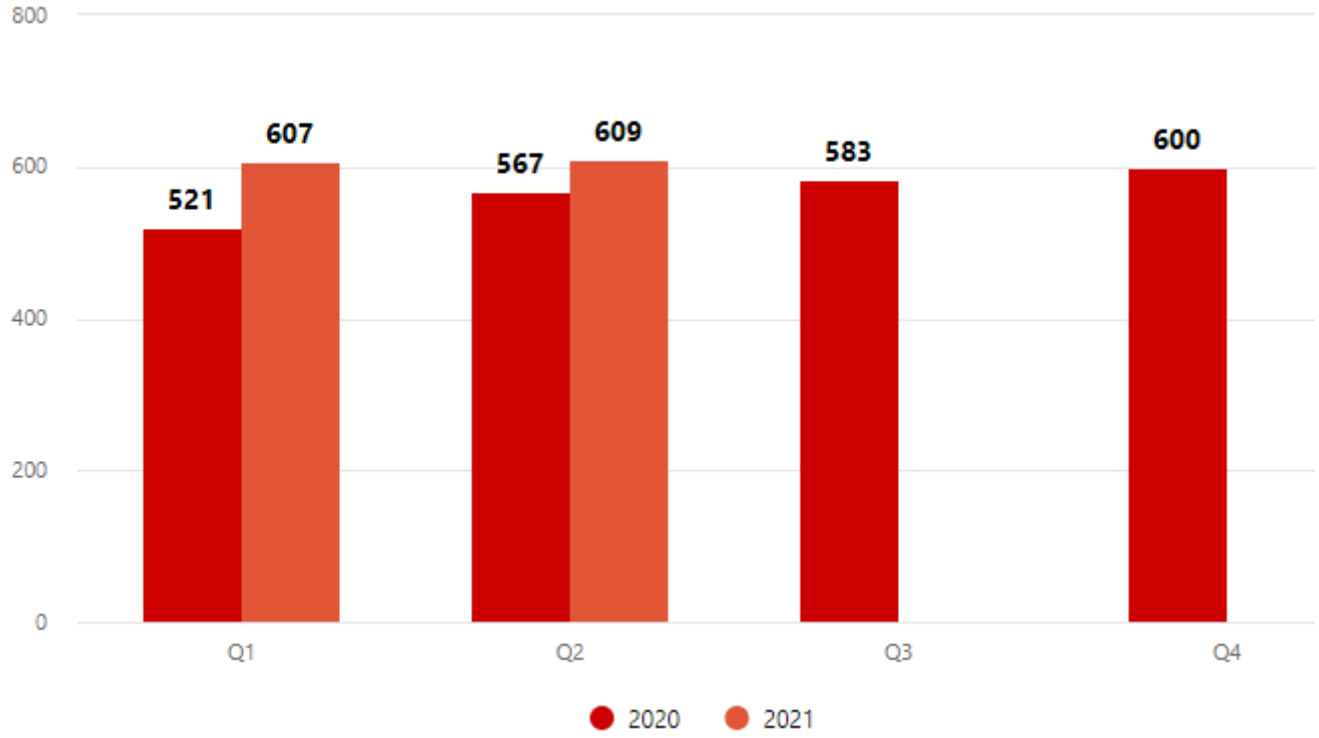

Рис.1.2. Кількість атак у 2020 та 2021 роках [5]

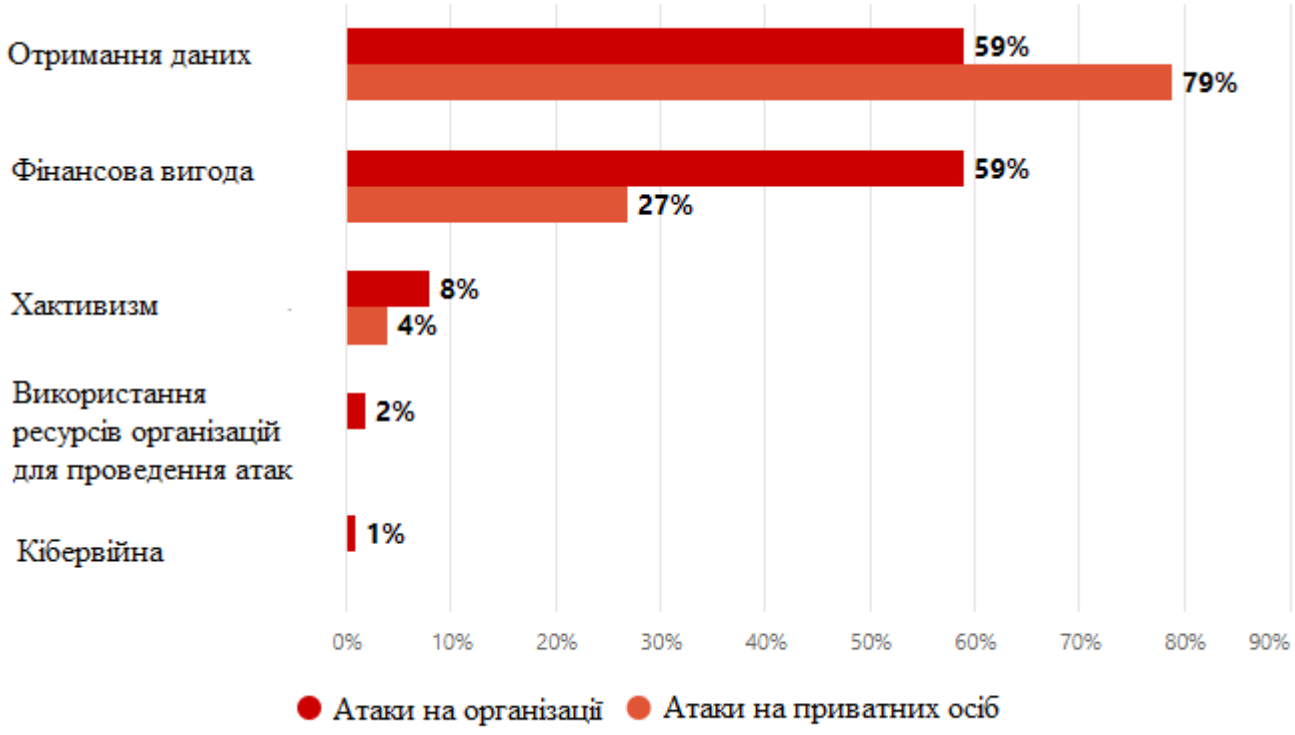

Рис.1.3. Наміри зловмисників [5]

Рис.1.4. Типи вкрадених даних (атаки на організації) [5]

Атаки з використанням ВПО зайняли перше місце серед кіберзлочинів. Порівняно з I кварталом 2021 року частка цього методу зросла на 15 процентних пунктів та становить 73%.

У II кварталі найвищі показники за кількістю атак з використанням шифрувальників склала 69% серед усіх атак з використанням ШПЗ. Піковий приріст відбувся у квітні. Проте на початку травня зловмисники атакували найбільшу трубопровідну систему США Colonial Pipeline та поліцію округу Колумбія, чим привернули увагу правоохоронних органів [5]. У результаті кіберзлочинці почали змінювати підходи до атак, а також вносити зміни до партнерських програм.

Частка атак, які припали на держустанови зросла з 12%, зафіксованих у I кварталі 2021 року, до 20% у II кварталі. У 73% інцидентів з використанням

шкідливого програмного забезпечення взяли участь зловмисники, які поширюють шкідливі програми - шифрувальники. Було виявлено новий завантажувач Tomiris, який було виявлено фахівцями PT ESC. Даний шифрувальник має функції для закріплення і відправляє зашифровану інформацію про робочі станції на підконтрольний зловмисникам сервер.

Кіберзагрози для торгової галузі зазнав змін. У II кварталі було відзначено, з одного боку, зменшення кількості атак типу Magecart, а з іншого — збільшення частки атак, у яких зловмисники використовували програми-вимагачі. Якщо раніше кіберзлочинці переслідували мотив крадіжки даних, то зараз вони намагаються отримати пряму фінансову вигоду від атак.

Промислова галузь цього кварталу також особливо часто страждала від програм-шифрувальників. Вони були виявлені в 80% інцидентів із використанням шкідливих даних. Почастішали випадки використання хакінгу: частка цього методу зросла з 29% до 34%. Фахівці PT ESC виявили нове шкідливе програмне забезпечення для віддаленого управління B-JDUN, помічене в атаці на енергетичну компанію [5].

Лідируючу позицію серед ВШ, що застосовується в атаках на організації, як і раніше, займають програми-вимагачі. До речі, частка атак із використанням таких програм за квартал зросла з 63% до 69%. У порівнянні з I кварталом більш ніж удвічі збільшилася частка атак з використанням завантажувачів.

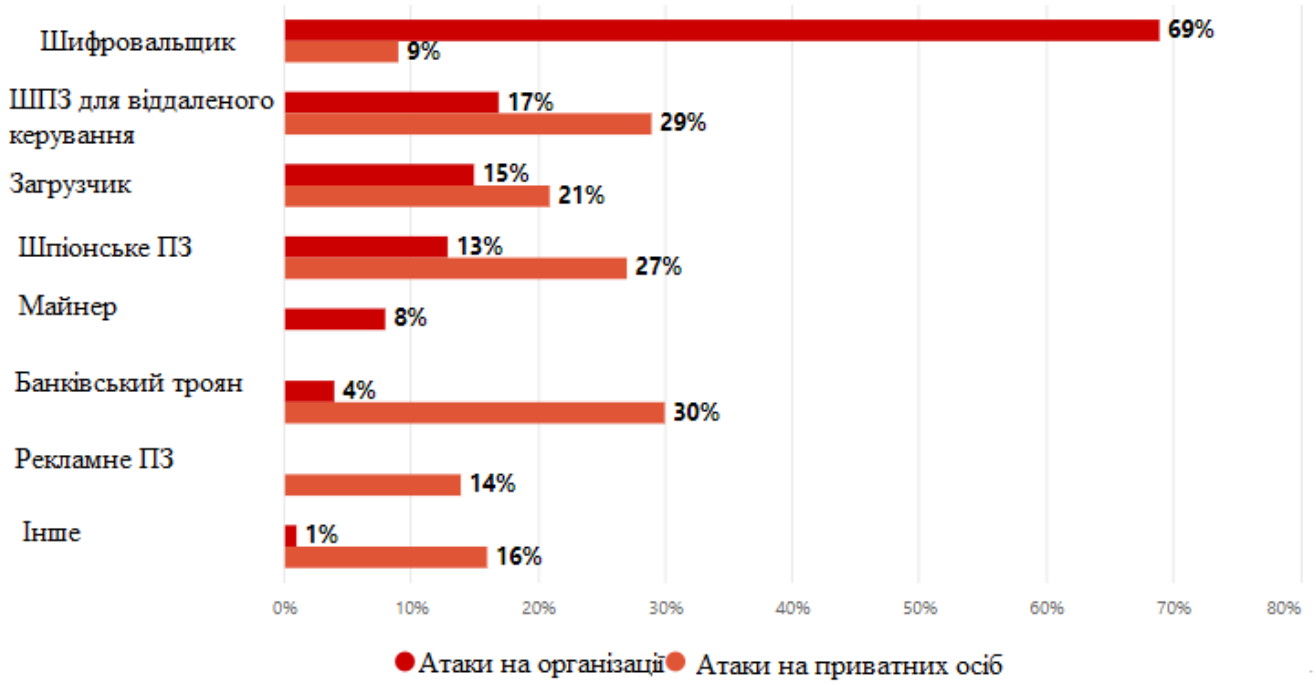

Рис. 1.5 Доля атак з використанням ШПЗ [5]

Основним способом поширення шкідливих атак на організації (58%) залишається електронна пошта. При цьому частка використання сайтів для поширення ШПЗ в організаціях зросла з 2% до 8%. Наприклад, цим способом скористалися зловмисники, які розповсюджують шпигунське програмне забезпечення, націлене на програмістів, які працюють з Node.js. Шкідливість імітував компонент Browserify в реєстрі npm.

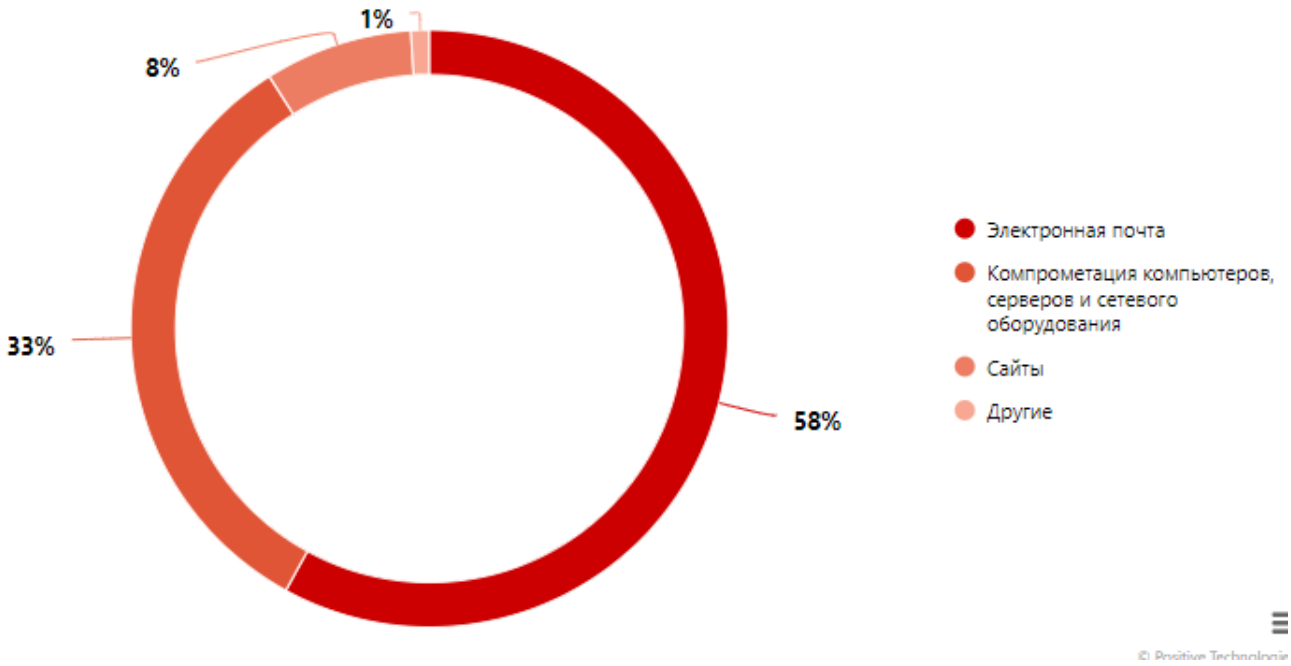

Рис.1.6. Способи поширення шкідливого ПЗ (частка атак на організації з використанням ВПЗ) [5]

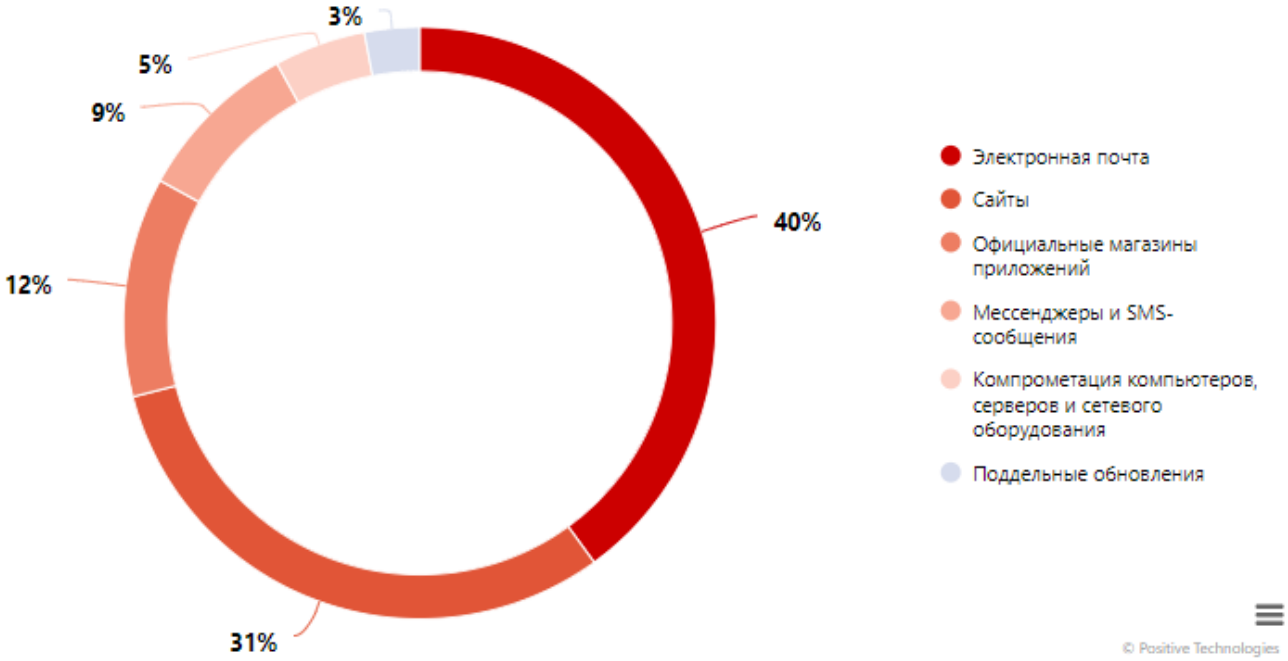

Рис.1.7. Способи поширення шкідливого ПЗ (частка атак на приватних осіб з використанням ВПЗ) [5]

Тож, як видно з звіту, велика частка атак відбувається через компроментацію серверного обладнання, комп’ютерів, мережевого обладнання. Тому надалі необхідно визначити технології, які необхідно застосовувати для захисту серверів організації.

1.4. Аналіз рішень технологій захисту файлового серверу організації

Кожна організація зберігає конфіденційні дані на файлових серверах, це файли та папки, які не повинні потрапляти в чужі руки. Кожен фахівець з кібербезпеки повинен зробити все можливе, щоб забезпечити цілісність даних, які там зберігаються. Визначимо головні вимоги щодо запобігання витоку даних з серверів організації.

1. Централізоване управління дозволами

Якщо компанія має децентралізований спосіб зберігання конфіденційних файлів і папок, фахвцям доведеться сканувати всю мережу, щоб знайти необхідні файли і змінити дозволи. Замість того, щоб розповсюджувати дані по різних комп'ютерах, IT-команди повинні консолідувати та зберігати всі свої файли та папки в одному місці. Централізоване керування дозволами гарантує, що ви можете швидко заблокувати переекспоновані дані та керувати дозволами для файлів та папок більш швидким та простим способом [6].

2. Обмеження розширених привілеїв для користувачів

Чим ширший портфель доступу співробітника до мережі, тим вищий ризик незвичайних подій доступу до файлового сервера. Занадто довгий список привілейованих користувачів може поставити під загрозу безпеку вашого домену. Найкраще рішення – обмежити кількість привілейованих користувачів на файлових серверах.

3. Відновлення Micro View на файлових серверах

Будь то зміна прав доступу користувача, виявлення незвичайної активності користувача або відстеження останніх прочитаних/змінених файлів чи папок, ці дії

відповідають мікродіючим подіям на файловому сервері. Можливість деталізувати складні деталі дозволяє IT-фахівцям швидко розпізнати складну активність файлового сервера та знайти причину проблеми.

4. Застосування практичного правила

Призначення ефективних дозволів на рівні загального ресурсу, NTFS та загальних дозволів може призвести до необмеженого доступу або навіть до повідомлень про відмову у доступі для користувачів, яким потрібний спільний доступ. Іншими словами, визначення та визначення ефективних дозволів гарантує, що ніхто не має надмірних прав доступу, які можуть поставити під загрозу ваші дані.

5. Адміністрація контролю за допомогою безпечного управління змінами

Практика безпечного керування змінами забезпечує повну видимість надмірних прав доступу, переекспонованих/застарілих даних, аномальних спроб доступу та іншого на ваших файлових серверах. Введіть безпечне керування змінами, щоб запобігти зловживанню зловмисниками своїми правами адміністратора.

6. Надавайте файлам та папкам короткі та інтуїтивно зрозумілі імена.

Довгі імена важче читати і ще важче перегортати, коли ви переглядаєте списки файлів та папок. Не забудьте також вибрати фразу, яка щось означає, коли ви називаєте один зі своїх файлів. Проте, називайте файли та папки простими та короткими заголовками.

7. Моніторинг ваших співробітників

Регулярний моніторинг систем ваших співробітників дозволяє вам відстежувати їхні повсякденні дії. Захистіть свої важливі файли, відстежуючи постійний обмін даними всередині організації. Більш того, ваш виділений файловий сервер відстежує дії кожного користувача та захищає вашу мережу від потенційних внутрішніх атак.

8. Захист від неавторизованих користувачів.

Користувачі з неавторизованим доступом до внутрішньої мережі можуть спробувати проникнути в систему, проникнути всередину, втрутитися або іншим

чином перехопити та спробувати змінити систему. По можливості рекомендується уникати адміністративних привілеїв, особливо, коли користувач має несанкціонований доступ до файлового сервера.

9. Контроль доступу до файлів

Обмеження доступу до файлів та папок для певних груп або окремих користувачів обмежує контроль від багатьох до кількох. Коли мова йде про запобігання експлуатації доступу до файлового сервера, ваша IT-група повинна регулярно перевіряти загальний доступ і безпеку, щоб не допустити зловмисників.

10. Використовувати функцію аудиту.

Коли доходить до аудиту змін файлів, краще діяти на випередження. Аудит файлового сервера - це простий спосіб відстежувати всі зміни, що відбуваються з важливими файлами та папками. Крім того, ви отримуєте єдиний журнал для однієї зміни, що відображає, хто, що, де і коли були внесені зміни до файлів і папок.

Розглянемо рішення захисту файлових серверів від світових компаній, які дозволяють компаніям захистити дані, які вони зберігають на файлових серверах.

Керуючись цих вимог проаналізуємо рішення захисту файлових серверів від таких потужних компаній як ESET та Imperva/

Рішення ESET Server Security

ESET Server Security забезпечує розширений захист даних компанії, що проходять через загальні сервери, мережеве сховище файлів, включаючи OneDrive, та багатоцільові сервери, надаючи безперервне ведення бізнесу. Дане рішення забезпечує:

захист від програм-вимагачів;

виявлення погроз нульового дня;

запобігання витоку даних;

захист від ботнету.

Основні переваги використання рішень ESET Server Security полягає в наступному.

Використання машинного навчання. Всі продукти ESET в даний час використовують машинне навчання у поєднанні з усіма іншими нашими рівнями захисту, і це відбувається з 1997 року. Зокрема, машинне навчання реалізується у вигляді обробки консолідованих вихідних даних та використання нейронних мереж.

Захист від програм-вимагачів. Додатковий рівень захисту користувачів від програм-вимагачів. Дана технологія відстежує та оцінює всі запущені програми на основі їх поведінки та репутації. Призначена для виявлення та блокування процесів, які нагадують своєю поведінкою програми-вимагачі.

Захист від атак мережі. ESET Network Attack Protection робить ефективним виявлення відомих вразливостей на мережному рівні. Рішення представляє собою рівень захисту від поширення шкідливих програм, мережевих атак та експлуатації вразливостей, для яких ще не випущено або розгорнуто патч.

Захист від ботнету. ESET Botnet Protection виявляє шкідливе з'єднання, яке використовується ботнетами, і в той же час ідентифікує шкідливі процеси. Будь-яка виявлена шкідлива комунікація блокується і відповідне повідомлення надсилається користувачеві.

Додатковий аналіз хмарної пісочниці. ESET Dynamic Threat Defense забезпечує ще один рівень безпеки для рішень ESET File Security за рахунок використання хмарної технології пісочниці для виявлення нових типів загроз, що ніколи раніше не зустрічалися.

Блокувальник експлойтів. ESET Exploit Blocker відстежує вразливі програми (браузери, програми для читання документів, поштові клієнти, Flash, Java та ін.). Замість просто фокусуватися на певні ідентифікатори CVE, він фокусується на методах реалізації експлойту. Під час спрацьовування загроза негайно блокується на машині.

Запобігання вторгненням – HIPS. Система запобігання вторгненням (HIPS) від ESET відстежує активність системи та використовує заздалегідь певний набір правил для розпізнавання та зупинення підозрілої поведінки системи.

Розширений сканер пам'яті. Advanced Memory Scanner від ESET відстежує поведінку шкідливого процесу та сканує його, як тільки він звільняється від блокування пам'яті. Безфайлові шкідливі програми не потребують постійних компонентів файлової системи, які можуть бути знайдені звичайним способом. Тільки сканування пам'яті може успішно виявити та зупинити такі шкідливі атаки.

Захист серверів Linux . ESET надає установники для найбільш популярних дистрибутивів систем на основі Unix, включаючи "готові" варіанти RedHat та SuSE, які відповідають стандарту File-System-Hierarchy. Не потребує жодних зовнішніх бібліотек, крім LIBC.

Сховище Office 365 OneDrive .Після реєстрації на окремому сервері ESET може сканувати OneDrive, щоб забезпечити відображення та моніторинг надійного сховища компанії.

AMSI / Захищена сервісна підтримка .У продуктах ESET використовується інтерфейс сканування захисту від шкідливих програм (AMSI) з метою забезпечення покращеного захисту від шкідливих програм для користувачів, даних, програм та робочих навантажень. Крім того, використовується захищений сервісний інтерфейс, який являє собою новий модуль безпеки, вбудований у Windows, що дозволяє завантажувати лише довірений підписаний код із покращеним захистом від атак шляхом впровадження коду.

Вбудована пісочниця .Вбудована в продукт пісочниця ESET допомагає виявити реальну поведінку об'єкта загрози, приховане під поверхнею замаскованого шкідливого ПЗ.

Використання рішення ESET Remote Administrator (ERA) — програми, яка дозволяє централізовано керувати продуктами ESET, встановленими в мережному середовищі. Система управління завданнями ESET Remote Administrator дозволяє встановити на віддалені комп'ютери рішення ESET для забезпечення безпеки та швидко реагувати на нові проблеми та загрози. ESET Remote Administrator не надає

захисту від шкідливого коду, а покладається на те, що на кожному клієнті встановлено і використовується рішення ESET.

У рішеннях ESET для безпеки передбачена підтримка мереж, що використовують кілька платформ різних типів. У мережі можуть співіснувати операційні системи Microsoft, Linux та Mac OS, а також системи, що працюють на мобільних пристроях (мобільні телефони та планшети).

Наведемо приклад архітектури мережі, захищеної рішеннями ESET для забезпечення безпеки. Цими рішеннями керує програма ERA.

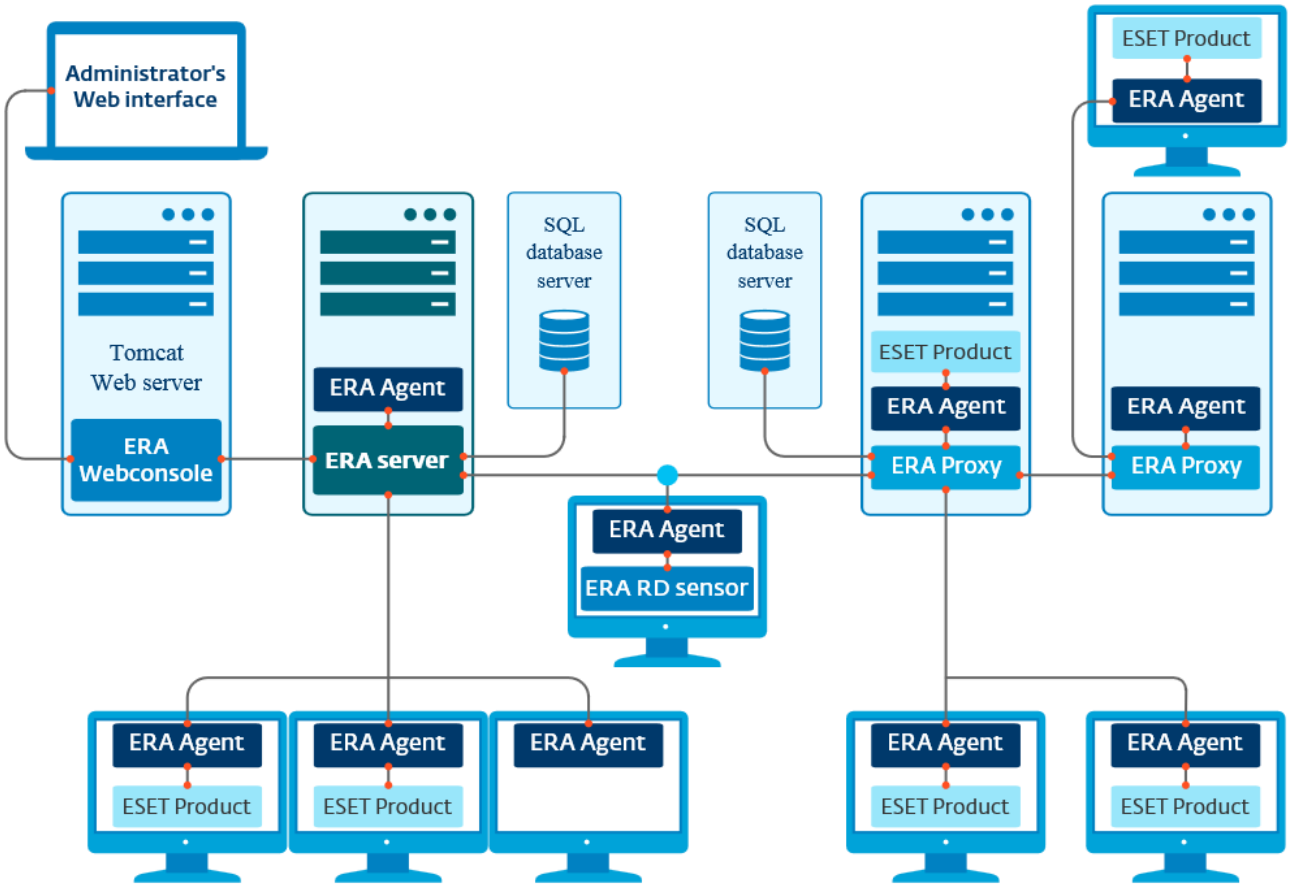

Рис.1.8. Архітектура мережі рішення ESET

Тож як видно з архітектури рішення ESET ERA дозволяє, завдяки використання агентів проводити моніторинг мережі для виявлення загроз як на кінцевих станціях, так і на серверах інформаційної системи організації.

Рішення захисту файлового сервера на ОС Microsoft Windows від шкідливих програм. Працює з урахуванням усіх особливостей серверного середовища. Він забезпечує безпеку персональних та платіжних даних, а також всіх даних CRM, поштових акаунтів, внутрішньої документації та файлів, що пересилаються. Продукт актуальний для великих компаній із мережею філій, міжнародних холдингів та банківських структур.

Зробимо аналіз забезпечення безпеки файлів рішенням Imperva.

Основні рішення Imperva:

SecureSphere File Activity Monitor;

SecureSphere File Firewall;

SecureSphere for SharePoint;

SecureSphere Directory;

Services Monitor;

User Rights Management for Files.

Традиційні підходи до аудиту операцій з файлами та управління правами доступу часто не відповідають потребам замовників. Інструменти адміністрування та інші поширені рішення від сторонніх постачальників, такі як групи в службах каталогів та вбудовані в операційну систему механізми аудиту файлів, не відповідають високим темпам зростання інформаційних систем та неструктурованих даних.

Продукти лінійки Imperva SecureSphere File Security забезпечують моніторинг, аудит та захист файлів на файлових серверах та мережевих сховищах (NAS), а також контроль прав доступу користувачів у реальному часі. Вони дозволяють організаціям налагодити стандартну процедуру для аналізу прав доступу, дозволяючи власникам даних приймати рішення на основі отриманої інформації. Ці рішення забезпечують

безпеку конфіденційних файлових даних шляхом оповіщення та при необхідності блокування спроб несанкціонованого доступу. Завдяки можливості створення чітких, достовірних звітів та інструментів аналітики можна оперативно розслідувати інцидент безпеки. На відміну від вбудованих механізмів, рішення SecureSphere виконують аудит доступу до файлів без впливу на продуктивність файлових серверів.

Продукти Imperva SecureSphere File Security дозволяють проводити:

• Аудит доступу всіх користувачів до файлів для забезпечення безпеки та відповідності стандартам, а також ефективності IT-операцій.

• Зіставлення файлів із власниками даних.

• Оптимізація аналізу прав доступу за рахунок надання керівництву фінансових або кадрових відділів можливості визначати користувачів, які матимуть доступ до службових файлів.

• Оповіщення про запити доступу до файлів, що порушують корпоративні політики, або їх блокування.

• Дотримання вимог стандартів та реагування на інциденти безпеки за допомогою розширених інструментів аналітики та звітності.

Можливості Imperva щодо безпеки файлів:

Аудит доступу до файлів та цілісність даних без зниження продуктивності ключових систем.

Підвищення ефективності IT-операцій

Пристрої SecureSphere дозволяють автоматизувати виконання найскладніших завдань з управління правами користувачів, аудиту доступу до даних та пошуку їх власників:

• об'єднання прав користувачів усередині організації;

• визначення способу отримання прав;

• комплексний облік операцій доступу;

• визначення власників даних та надання їм можливості керувати

правами доступу до файлів;

• відображення змін користувачів та груп у службі Active Directory;

• пошук даних, що не використовуються;

• спрощене перенесення даних та консолідація доменів.

Рішення SecureSphere здійснюють безперервний моніторинг та аудит усіх операцій із файлами в реальному часі без зниження продуктивності та доступності файлових серверів. Вони створюють докладний журнал аудиту, який містить імена користувачів, файлів, тек, час доступу, найменування операцій та інші параметри. Можливість виявлення змін файлів та оповіщення про ці зміни допомагає організаціям дотримуватись стандартів, а також виконувати вимоги модуля File Integrity.

Monitoring у частині безпеки. Журнал аудиту зберігається у зовнішньому, захищеному сховищі, доступному тільки для читання та лише на основі ролей. Це дозволяє реалізувати принцип розподілу обов'язків.

Контроль прав доступу користувачів до файлів. Пристрої SecureSphere визначають поточні права доступу користувачів до файлів та за допомогою комплексного циклу аналізу реалізують принцип доступу до важливої інформації лише за наявності службової потреби. Цей механізм дозволяє оптимізувати аудит та контроль дозволів шляхом консолідації прав доступу до файлів на файлових серверах та мережевих сховищах NAS, а також створення відповідних звітів. Циклічна перевіряння прав користувачів має на увазі:

• визначення користувачів, які мають доступ до файлів із конфіденційними даними;

• оповіщення про користувачів із надмірними правами доступу;

• виявлення неактивних користувачів та невикористовуваних прав доступу;

• забезпечення послідовних операцій з аналізу прав доступу;

• відстеження змін у службі Active Directory та сповіщення про них у реальному часі.

Контроль доступу до файлів, здійснюваний власниками даних

Пристрої SecureSphere визначають власника даних шляхом аналізу його роботи з даними. Організації можуть знижувати ризик та забезпечувати захист файлів, безпосередньо залучаючи власників даних до аналізу прав доступу.

Система SecureSphere забезпечує доступ до зручного порталу для власників даних, на якому керівники підприємства можуть реєструватися, приймати рішення про доступ до файлів та надсилати результати безпосередньо до IT-відділу для вжиття заходів. Надаючи можливість прийняття рішень про контроль прав доступу до файлів саме тим особам, які мають найповнішу інформацію (тобто керівникам фінансових або кадрових відділів), рішення SecureSphere дозволяють виконувати аналіз прав доступу регулярніше і точніше. Завдяки прозорій процедурі операцію аналізу можна проводити досить часто, забезпечуючи захист важливих даних та відповідність стандартам.

Оповіщення про несанкціоновані дії та їх блокування у реальному часі.

Пристрої SecureSphere розширюють стандартні повноваження, блокуючи доступ до файлів або сповіщаючи про порушення корпоративної політики. Блокування доступу на основі політики дозволяє організаціям забезпечити захист від помилок, пов'язаних із правами доступу та виникаючих на рівні каталогів та файлів. Гнучка система дає можливість враховувати при створенні політик різні критерії, наприклад метадані файлів, контекст організації, операції доступу і класифікацію даних, а потім вживати необхідних заходів при виявленні небажаних дій.

Розслідування інцидентів безпеки та вжиття заходів

Рішення SecureSphere надають інтерактивні засоби аналітики аудиту, що дозволяють виводити на екран відомості про доступ до даних, зміни в Active Directory та права користувачів за допомогою кількох клацань миші. Використовуючи ці дані, фахівці служб безпеки, нормативної відповідності та аудиту можуть визначати тенденції, механізми та ризики, пов'язані з операціями з файлами та правами користувачів.

Можливість оперативно переглядати дані аудиту в багатовимірному режимі, а також інтерактивні інструменти аналітики полегшують виявлення інцидентів безпеки та їх розслідування.

Швидка та ефективна реєстрація дотримання стандартів за допомогою графічних звітів.

Пристрої SecureSphere пропонують широкі можливості для створення графічних звітів, що дозволяють підприємствам оцінювати ризики та реєструвати дотримання вимог стандартів безпеки, таких як SOX, PCI, HIPAA та інших законів про конфіденційність даних. Можна переглядати звіти у будь-який момент, а також налаштувати для них графік створення та розсилки. Панель моніторингу в реальному часі дає загальну картину про події у системі безпеки та стан системи. Система звітності SecureSphere миттєво виводить на екран відомості про поточні проблеми, пов'язані з безпекою, дотриманням стандартів та правами користувачів.

Моніторинг та захист Microsoft SharePoint

Рішення SecureSphere for SharePoint гарантує захист конфіденційних файлів організацій у системі SharePoint. Він враховує унікальні вимоги щодо безпеки файлів, веб-додатків та баз даних SharePoint, надаючи користувачам доступ лише за наявності обґрунтованої службової необхідності. Рішення забезпечує моніторинг та аналіз прав доступу та використання даних, а також захист від інтернет-загроз.

• Застосування бізнес-правил за допомогою оповіщення або блокування доступу до файлів у системі SharePoint.

Надання прав доступу з можливістю перегляду актуальних та точних відомостей про власників даних та повноваження.

• Виявлення файлів, запити доступу яких давно не подавалися.

• Прискорення перенесення даних та консолідація доменів у службах каталогів на основі інформації про власників даних, неактивних облікових записів та даних, що не використовуються.

• Оптимізація аналізу прав користувачів у процесі перенесення та консолідації даних.

Моніторинг змін у Active Directory

Служба Active Directory відіграє ключову роль при визначенні прав доступу до SharePoint, файлових серверів та пристроїв NAS. Тому будь-які зміни в Active Directory можуть значно вплинути на конфіденційні бізнес-дані. Рішення SecureSphere Directory Services Monitor (DSM) допомагає організаціям забезпечити безпеку та дотримання стандартів під час роботи зі службою Microsoft Active Directory. Воно дозволяє ефективно контролювати виконання найважливіших завдань, таких як поділ обов'язків, відстеження дій привілейованих користувачів, підвищення привілеїв та внесення суттєвих змін. SecureSphere Directory Services Monitor дає можливість безперервно відстежувати дії в службах каталогів, гарантуючи безпеку та відповідність вимогам стандартів, а також надає IT-фахівцям функції аудиту, оповіщення, аналізу змін, складання звітів та реагування в реальному часі.

Пристрої SecureSphere мають найкращі серед аналогів можливості для аудиту доступу до файлів та управління правами доступу користувачів, допомагають дотримуватися вимог стандартів безпеки, забезпечуючи високий рівень захисту та оптимізуючи IT-операції. Ефективно використовуючи функції централізованого керування та звітності, рішення SecureSphere відповідають вимогам замовників будь-якого масштабу – від невеликих організацій з одним файловим сервером чи системою SharePoint до великих підприємств із розподіленою мережею ЦОД. Ці рішення забезпечують неперевершену безпеку даних.

Тож SecureSphere File Security у сфері безпеки даних показує кращі можливості. І для наступних досліджень розглянемо архітектуру даного рішення для захисту файлових серверів інформаційної системи організації.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ФАЙЛОВИХ СЕРВЕРІВ ОРГАНІЗАЦІЇ

2.1. Визначення завдань захисту файлових сервері організації

Кожна організація зберігає конфіденційні дані на файлових серверах; файли та папки. Ці дані можуть потрапляти в чужі руки. Як IT-фахівцеві з кібербезпеки потрібно робити все можливе, щоб забезпечити цілісність даних. Визначимо деякі з наших кращих порад щодо запобігання витоку даних.

1. Централізоване управління дозволами

Якщо компанія має децентралізований спосіб зберігання конфіденційних файлів і папок, IT-менеджерам доведеться сканувати всю мережу, щоб знайти необхідні файли і змінити дозволи. Замість того, щоб розміщувати дані на різних комп'ютерах, IT-команди повинні консолідувати та зберігати всі свої файли та папки в одному місці. Централізоване керування дозволами гарантує, що ви можете швидко заблокувати переекспоновані дані та керувати дозволами для файлів та папок більш швидким та простим способом.

2. Обмеження розширених привілеїв для користувачів

Чим ширший портфель доступу співробітника до мережі, тим вищий ризик незвичайних подій доступу до файлового сервера! Занадто довгий список привілейованих користувачів може поставити під загрозу безпеку вашого домену. Найкраще рішення – обмежити кількість привілейованих користувачів на ваших файлових серверах.

3. Відновлення Micro View на файлових серверах

Будь то зміна прав доступу користувача, виявлення незвичайної активності користувача або відстеження останніх прочитаних/змінених файлів чи папок, ці дії відповідають мікродіючим подіям на файловому сервері. Можливість деталізації складних деталей дозволяє IT-фахівцям швидко розпізнати складну активність файлового сервера та знайти причину проблеми.

4. Застосування практичного правила

Призначення ефективних дозволів на рівні загального ресурсу, NTFS та загальних дозволів може призвести до необмеженого доступу або навіть до повідомлень про відмову у доступі для користувачів, яким потрібний спільний доступ. Іншими словами, визначення та визначення ефективних дозволів гарантує, що ніхто не має надмірних прав доступу, які можуть поставити під загрозу ваші дані.

5. Адміністрація контролю за допомогою безпечного управління змінами

Практика безпечного керування змінами забезпечує повну видимість надмірних прав доступу, переекспонованих/застарілих даних, аномальних спроб доступу та іншого на ваших файлових серверах. Введіть безпечне керування змінами, щоб запобігти зловживанню зловмисниками своїми правами адміністратора.

6. Надавайте файлам та папкам короткі та інтуїтивно зрозумілі імена.

Довгі імена важче читати і ще важче перегортати, коли ви переглядаєте списки файлів та папок. Не забудьте також вибрати фразу, яка щось означає, коли ви

називаєте один зі своїх файлів. Проте, називайте файли та папки простими та короткими заголовками.

7. Моніторинг ваших співробітників

Регулярний моніторинг систем ваших співробітників дозволяє вам відстежувати їхні повсякденні дії. Захистіть свої важливі файли, відстежуючи постійний обмін даними всередині організації. Більш того, ваш виділений файловий сервер відстежує дії кожного користувача та захищає вашу мережу від потенційних внутрішніх атак.

8. Захист від неавторизованих користувачів.

Користувачі з неавторизованим доступом до внутрішньої мережі можуть спробувати проникнути в систему, проникнути всередину, втрутитися або іншим чином перехопити та спробувати змінити систему. По можливості рекомендується уникати адміністративних привілеїв, особливо, коли користувач має несанкціонований доступ до файлового сервера.

9. Контроль доступу до файлів

Обмеження доступу до файлів та папок для певних груп або окремих користувачів обмежує контроль від багатьох до кількох. Коли мова йде про запобігання експлуатації доступу до файлового сервера, ваша IT-група повинна регулярно перевіряти загальний доступ і безпеку, щоб не допустити зловмисників.

10. Використовуйте функцію аудиту.

Коли справа доходить до аудиту змін файлів, краще виявляти ініціативу. Аудит файлового сервера - це простий спосіб відстежувати всі зміни, що відбуваються з вашими важливими файлами та папками. Крім того, ви отримуєте єдиний журнал для однієї зміни, що відображає, хто, що, де і коли були внесені зміни до файлів і папок.

Отже, якщо ви хочете підвищити безпеку критично важливих файлів та папок на вашому файловому сервері, SecureSphere File Security може стати для вас рішенням. Це рішення для аудиту файлового сервера допомагає вам повідомляти про спроби створення, модифікації, видалення або зміни дозволів файлу чи папки.

2.2. Призначення та архітектура захисту файлових серверів SecureSphere

Рішення SecureSphere File Security захищають конфіденційні файли на файлових серверах, пристроях зберігання та репозиторіях вмісту. SecureSphere забезпечує повну прозорість володіння даними, їх використання та прав доступу, а також дозволяє керівникам, аудиторам, спеціалістам з безпеки та IT-менеджерам підвищувати безпеку даних та дотримуватись нормативних вимог.

SecureSphere допомогає:

Проводити аудит доступу до конфіденційних файлів з боку привілейованих користувачів та користувачів додатків.

Попереджати або блокувати запити на доступ до файлів, які порушують корпоративні політики.

Прискорює реагування на інциденти та розслідування за рахунок централізованого управління та розширеної аналітики.

Архітектура системи SecureSphere (рис.2.1) складається з наступних компонентів:

шлюзу моніторингу та безпеки;

серверу керування.

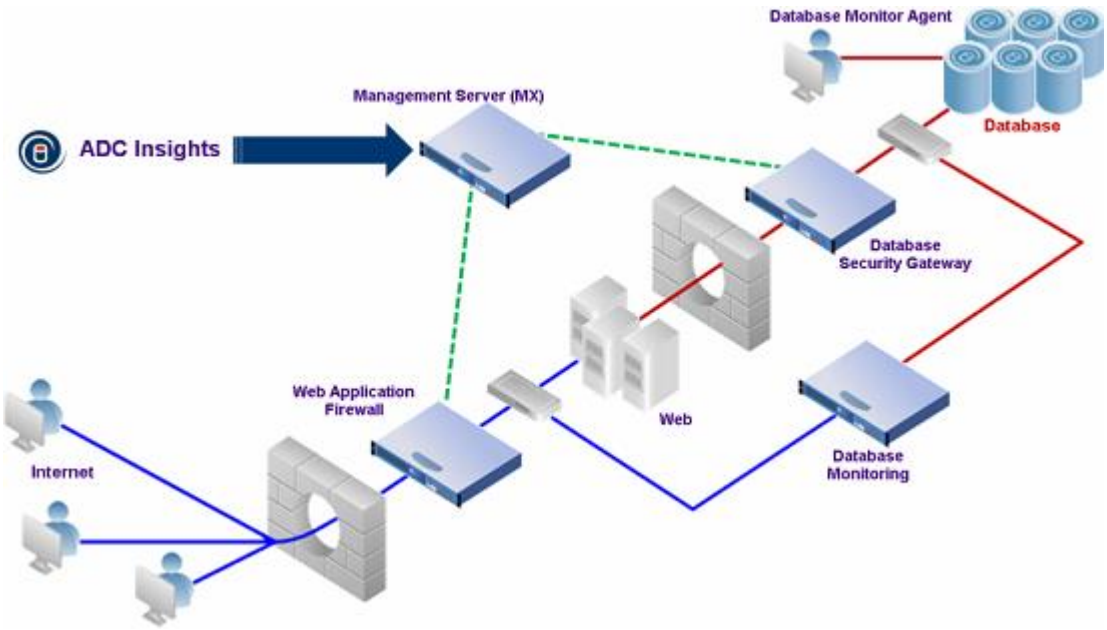

Рис.2.1. Архітектура системи SecureSphere

Шлюз моніторингу та безпеки виконує моніторинг додатків та даних, забезпечуючи повну видимість того, як ці дані фактично використовуються на підприємстві, незалежно від того, чи отримують вони прямий чи опосередкований доступ через додатки. Він також виконує повний спектр моніторингу активності баз даних, файлових серверів та програм та блокує шкідливий трафік.

Сервер керування (MX) надає інструмент централізованого керування для 15 шлюзів SecureSphere, що дозволяє виконувати великомасштабні розгортання у розподілених середовищах.

SecureSphere дозволяє створити модель мережі організації, а потім використовувати цю модель для управління відкриттям сервісів і даних, оцінки виявлених сервісів і моніторингу активності у вашій базі даних. Це досягається шляхом створення моделі мережі в SecureSphere, що включає наступні елементи:

Сайти : фізичний сайт, на якому встановлені групи серверів (наприклад, центри обробки данных).

Групи серверів: контейнер, який дозволяє вам логічно представити вашу систему, наприклад, ви можете побудувати сервери різних груп для різних географічних місць. Групи серверів містять фізичні сервери, служби та фактичні додатки.

Для FAM кращою практикою є те, що група серверів представляє собою єдине сховище. Віно може включати більше одного сервера в кластер або більше одного IP-адреса одного сервера, але не різні файлові сервери.

Служби: можуть містити файлові продукти, служби CIFS або NFS.

SecureSphere пропонує ряд основних функцій, що стосуються всіх аспектів діяльності файлових служб. Доступні функції включають таке:

Application Defense Center (ADC)

Політики

Моніторинг

Аудит

Складання звітів

Відстеження користувачів

ADC. Експерти з кібербезпеки в Центрі захисту програм Imperva (ADC) гарантують, що SecureSphere завжди в курсі останніх досягнень захисту від нових загроз, а також останніх передових методів забезпечення відповідності нормативним вимогам.

Дослідження ADC базується на кількох джерелах даних та зосереджено на таких питаннях:

- Аналіз поведінки програм, будь то упаковані програми, такі як SAP або Oracle E-Business Suite, або програми користувача, такі як PHP або AJAX.
- Внутрішнє дослідження реалізацій баз даних для виявлення вразливостей безпеки (наприклад, кілька вразливостей, виявлених ADC, було підтверджено та виправлено Oracle).

- Збір інформації про виявлені в системі вразливості та виправлення, випущені постачальниками.
- Передові методи безпеки розроблені для баз даних, включаючи консультації з органами за галузевими стандартами.
- Забезпечення SecureSphere найсучаснішими засобами захисту, включаючи оновлення сигнатур, профілі попереджень, профілі аудиту та звіти. Підписи ідентифікують відомі атаки. ADC підтримує словники з кількома тисячами сигнатур, деякі з яких спочатку були надані Snort®, інші розроблені самим ADC.

Політики

Політики безпеки захищають від більшості відомих атак та погроз. В системі SecureSphere надається велика кількість політик за замовчанням. Адміністратори можуть змінювати існуючі політики та створювати нові.

Політики аудиту надають інструменти для аудиту та відповідності. Використовуючи ці політики, адміністратори можуть у реальному часі створювати звіти про різні дії з базою даних, попередження про підозрілі дії та звіти про відповідність. Адміністратори можуть змінювати існуючі політики та створювати нові.

На додаток до політик безпеки та аудиту SecureSphere надає набори дій та виконувані дії , які визначають дії, що здійснюються SecureSphere при виконанні певних умов. Набори дій налаштовуються, а потім приєднуються як наступні дії до різних елементів SecureSphere, таких як політики безпеки, системні події, політики аудиту, звіти, архівування, активні модулі, завдання і т.д.

Моніторинг

Моніторинг SecureSphere інформує адміністраторів про всі події Active Directory і дозволяє зрозуміти ризик, пов'язаний з підозрілою активністю.

Він чітко відображає згенеровану інформацію у центральному місці. Інформація, що генерується в режимі реального часу, включає системні події,

попередження, порушення, статус шлюзу, системні попередження та інформацію про архівування.

SecureSphere автоматично об'єднує пов'язані події безпеки, зіставляючи їх в інтуїтивно зрозумілих попередженнях, які класифікують дії, пов'язуючи їх із відомими атаками, та інформує адміністраторів про цю інформацію. Крім того, монітор SecureSphere інформує вас про системні події, такі як вхід у систему та вихід з неї, а також про помилки або попередження, пов'язані з системою (наприклад, про перевищення визначених граничних значень).

Аудит

SecureSphere надає комплексні можливості аудиту, дозволяючи налаштовувати політики аудиту, які визначають, які дані підлягають аудиту, а потім відображати перевірені дані у вигляді зручних для читання графіків, які розбивають перевірені дані на звіти, що легко читаються, на основі безлічі факторів, таких як відстежувані сервери, різні типи користувачів, аспекти, пов'язані з запитами, та багато іншого. SecureSphere додатково може інтегруватися із зовнішніми системами керування інформацією та подіями безпеки (SIEM), щоб включити ці системи в робочий процес керування даними.

Складання звітів

SecureSphere включає надійний механізм звітності , який дозволяє створювати заздалегідь визначені або визначені користувачем звіти на основі накопичених даних, які можуть бути створені або автоматично, або на в реальному часі, або за розкладом для регулярного виконання, а потім розподілятися при необхідності.

Адміністратори можуть використовувати можливості автоматичної звітності для реалізації робочого процесу, який допомагає регулярно аналізувати найсвіжіші загрози. Наприклад, можна запланувати SecureSphere для автоматичного створення звіту на початку кожного тижня, в якому перераховані всі нові таблиці конфіденційних даних, виявлених у мережі, а потім автоматично надіслати цей звіт адміністратору баз даних електронною поштою, одночасно створюючи завдання

перевірки SecureSphere, призначене адміністратору баз даних. Адміністратор бази даних вивчає звіт і може визначити, чи слід створювати нові дані керівним принципам для конфіденційних даних у вашій мережі, а потім позначає завдання як закрите. Крім того, завдання можна налаштувати автоматичне оновлення диспетчера при зміні статусу завдання.

Відстеження користувачів

Функція універсального відстеження користувачів (UUT- Universal User Tracking) SecureSphere підвищує безпеку та аудит, аналізуючи трафік, щоб точно пов'язувати користувачів зовнішнього інтерфейсу програми із запитами до бази даних.

Ідентифікація користувача надається в попередженнях та звітах аудиту, а політики безпеки для обмеження доступу до конфіденційних баз даних можуть бути включені для кожного користувача. UUT забезпечує готову підтримку корпоративних додатків, таких як Oracle E-Business Suite, SAP, PeopleSoft та інших, а також користувацьких додатків та додатків власної розробки.

3. РОЗРОБКА ВАРІАНТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФАЙЛОВОГО СЕРВЕРУ НА БАЗІ РІШЕННЯ SECURESPHERE FILE SECURITY

3.1. Розробка варіанту технології безпеки інфраструктури організації на базі рішення SecureSphere

SecureSphere складається з двох основних компонентів: шлюзу та сервера управління (MX). Захист в реальному часі є основним завданням шлюзу, в той час як основні ролі MX полягають у налаштуванні системи, зборі подій зі шлюзу, їх аналізі та відображенні попереджень, що виникають.

SecureSphere Gateway – це критично важливий компонент: у разі відмови шлюзу веб-сервери та сервери баз даних за шлюзом більше не захищені. З іншого боку, якщо SecureSphere MX виходить з ладу, захист не переривається.

Збій MX, що триває протягом тривалого часу, вплине на рівень захисту, який забезпечують SecureSphere Gateways, з наступних причин:

Профільування : Профільування програм MX виконується на основі даних, зібраних зі шлюзів.

Політики та профілі: не можна змінювати існуючі профілі або політики.

Сповіщення: шлюз передає події в MX, який зберігає та аналізує їх та відображає сповіщення, отримані з подій. Якщо підключення до MX відсутнє, шлюз зберігає події локально для подальшої передачі, але зрештою шлюз перезапише старіші події, оскільки доступний дисковий простір вичерпано. Коли підключення до MX відновлено та шлюз передає свій накопичений архів подій у MX, MX матиме неповні дані. Крім того, попередження, які зазвичай надсилаються заздалегідь визначеним одержувачам електронною поштою, тепер залишаються непоміченими.

Аудит: файли даних аудиту займають багато місця. Файли аудиту зберігаються на шлюзі, але якщо не архівувати регулярно (завдання MX), нові дані аудиту

губляться.

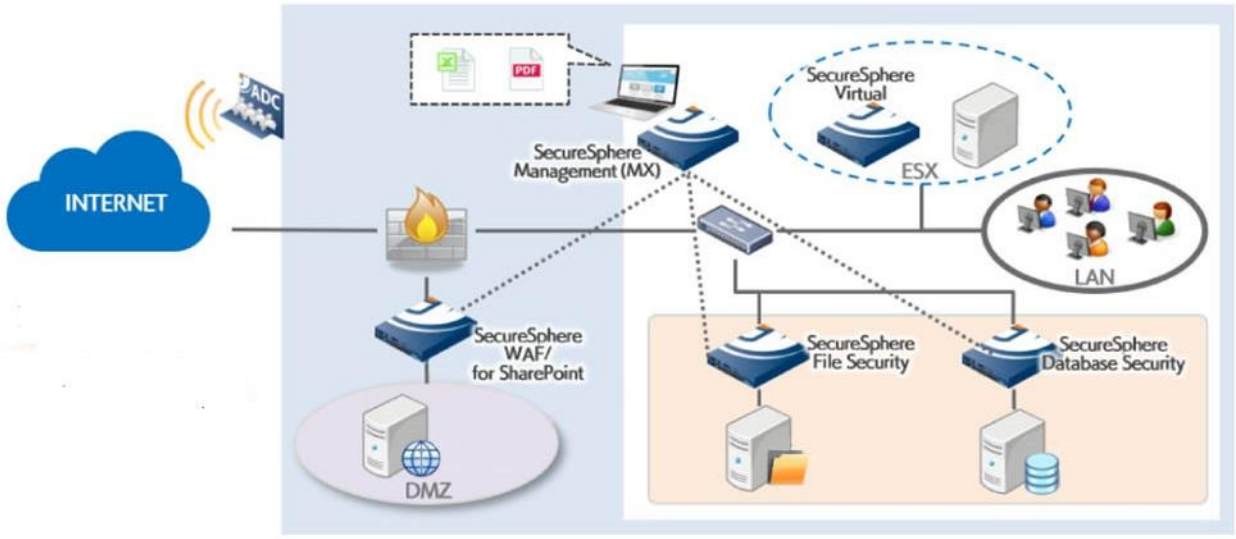

Рис. 3.1. Варіант архітектури захисту інфрастуктури організації [8]

Функція MX-High Availability використовує надлишкові MX у повністю автоматичній реалізації перемикання при відмові в активному/резервному стані, що не потребує втручання користувача. Система виявляє втрату активного MX і запускається механізм аварійного перемикання.

MX-HA підтримується як для спільно розміщених MX (один і той же центр обробки даних), так і для MX, розташованих у різних центрах обробки даних, проте необхідно враховувати два обмеження:

Обидва MX використовують одну і ту ж IP-адресу, коли стають активними (плаваюча IP-адреса), тому вони повинні знаходитися в одній і тій же LAN або віртуальній LAN, тому у разі віддалених центрів обробки даних VLAN має проходити через WAN/Інтернет.

Мінімальна пропускна здатність мережі 50 Мбіт/с має бути доступна для протоколів MX-HA для надійного та своєчасного функціонування та конвергенції.

До рішення Management Server-High Availability включені такі компоненти:Linux Heartbeat

Oracle Standby Database (Data Guard)

SecureSphere Server

Проверка працездатності HA

Imperva Watchdog

Linux heartbeat – це утиліта Linux, яка дозволяє реалізувати активно-пасивні кластери. Тактовий сигнал – це серце MX-HA, яке відповідає за базу даних та MX, а також за те, де вони виконуються.

Конфігурація Heartbeat включає такі ресурси:

Віртуальна IP-адреса (VIP)

Сервер бази даних

Сервер SecureSphere

Після запуску тактового сигналу, всі ресурси виділяються конкретному MX.

Heartbeat щохвилини перевіряє стан ресурсів. Якщо один із ресурсів не запускається на MX, всі ресурси перезапускаються на тому самому MX. Якщо перезапуск не вдалося, ініціюється аварійне перемикання.

Синхронізація бази даних базується на резервній базі даних Oracle (або Data Guard). Після встановлення MX-HA база даних на первинному MX налаштовується для підтримки резервної бази даних Oracle. База даних на вторинному MX видаляється та копіюється з первинного сервера як резервна база даних.

Після встановлення резервна база даних постійно синхронізується з основною базою даних за допомогою рішення Oracle.

SecureSphere Management Server є одним із ресурсів у системі, але він не змінюється під час встановлення MX-HA.

Щоб переконатися, що все гаразд, існує механізм перевірки працездатності, який перевіряє обидва сервери. Серце цього механізму - healthCheck.sh сценарій.

Сценарій Imperva Watchdog перевіряє статус роботи мережі і, якщо він недійсний, перезапускає серцебиття. Imperva Watchdog перевіряє роботу лише після успішного запуску MX-HA impctl. Якщо MX-HA зупинено вручну, видаляється зі списку спостереження сторожового таймера.Елементи, які необхідно виконати перед встановленням Management Server у режимі високої доступності (MX-HA), і включають:

Вимоги до апаратного та програмного забезпечення;

Відкриті порти для MX-HA;

Завдання перед встановленням.

У MX-HA приватна мережа, яка пов'язує два сервери MX, використовується для постійного копіювання інкрементних змін бази даних та файлів. Крім того, під час встановлення, а іноді й в інший час, усі дані бази даних мають бути передані цією мережею. Хоча мінімальної необхідної смуги пропускання не існує, рекомендується, щоб мережне з'єднання між ними було надійним, швидким і досить швидким, щоб обробляти необхідний обсяг трафіку для вашого розгортання.

Для забезпечення високої доступності Management Server High Availability (MX-HA) потрібна певна конфігурація обладнання та програмного забезпечення, яка включає:

Два MX-MX-High Availability не можуть бути встановлені на шлюзах.

Необхідно використати ліцензії на обидва сервери.

Обидва сервери керування у парі MX-HA мають бути однієї моделі пристрою (наприклад, обидва MX у парі MX-HA мають бути M160).

Фізичні та віртуальні моделі обладнання не можуть працювати разом у MX-HA. Наприклад, віртуальний сервер управління VM150 не може працювати разом з фізичним сервером управління M160 у MX-HA.

Обидва сервери повинні мати однаковий обсяг пам'яті (RAM) та дискового простору.

На обох серверах має бути встановлена та сама версія SecureSphere.

Кожен сервер повинен мати наступні два мережеві інтерфейси:

Інтерфейс для публічної мережі.

Інтерфейс для міжз'єднання (з використанням перехресного кабелю Ethernet при прямому підключенні або з використанням іншого кабелю, якщо потрібно при підключенні через інший пристрій) з іншим сервером. Цей інтерфейс використовується sycnhevtynfvb Linux та Oracle для синхронізації резервної бази даних.

Щоб MX-HA синхронізувалася між серверами керування, що входять до складу середовища MX-HA, необхідно щоб між двома серверами керування відкриті такі порти:

Ping: ICMP

SSH: 22 TCP

Oracle: 1521 TCP

Heartbeat: 5405 UDP.

Перед встановленням Management Server у режимі високої доступності необхідно виконати нижченаведені кроки.

Встановіть останній патч

Налаштувати взаємозалежні інтерфейси. Взаємопов'язана мережа має бути визначена під час процедури першого входу до системи на MX шляхом налаштування інтерфейсів LAN. Якщо цього не було зроблено під час першого входу до системи, тепер інтерфейси LAN можна налаштувати за допомогою impcfg.

Протестуйте взаємопов'язані інтерфейси. Щоб протестувати взаємопов'язані інтерфейси:

1. Надішліть відгук від першого MX до другого MX на його внутрішньому інтерфейсі.

2. Пінг не буде виконано, тому що MX блокує ICMP за промовчанням.

3. Відразу після перевірки зв'язку виконайте *arp -a* і знайдіть запис *arp* іншого сервера.

4. Якщо запис *arp* має допустиму MAC-адресу для іншого сервера, з'єднання було успішно налаштоване.

Завантажте RPM та підготуйте основний MX.

3.2 Система шифрування даних Venafi Encryption Director

Безпека транспортного рівня (TLS) [9]. Сертифікати серверів мають вирішальне значення для безпеки як доступних в Інтернеті, так і приватних веб-служб. Велика чи середня організація може мати тисячі чи навіть десятки тисяч таких сертифікатів, кожен із яких ідентифікує конкретний сервер у його середовищі. Незважаючи на критичну важливість цих сертифікатів, у багатьох організаціях відсутня формальна програма управління сертифікатами TLS та можливість централізованого моніторингу та управління своїми сертифікатами. Натомість управління сертифікатами має тенденцію поширюватися на кожну з різних груп, відповідальних за різні сервери та системи в організації. Центральні служби безпеки намагаються забезпечити належне управління сертифікатами кожної з цих розрізнених груп. Там, де немає централізованої служби управління сертифікатами, організація наражається на ризик, тому що після розгортання сертифікатів необхідно підтримувати поточні запаси для підтримки регулярного моніторингу та обслуговування сертифікатів. Організації, які не керують своїми сертифікатами належним чином, стикаються зі значними ризиками для своєї основної діяльності, включаючи:

- збої додатків, викликані простроченими сертифікатами сервера TLS

- приховане вторгнення, крадіжка, розкриття конфіденційних даних або інші атаки, що виникають внаслідок зашифрованих загроз або імітації сервера

- ризик аварійного відновлення, що вимагає швидкої заміни великої кількості сертифікатів та закритих ключів у відповідь на компрометацію центру сертифікації або виявлення вразливостей у криптографічних алгоритмах чи бібліотеках.

Незважаючи на критично важливий характер сертифікатів серверів TLS, багато організацій не визначили чітких політик, процесів, ролі та обов'язків, необхідних для ефективного управління сертифікатами. Більш того, багато організацій не використовують доступні інструменти автоматизації для підтримки ефективного управління числом сертифікатів, що постійно зростає. Наслідком є постійна вразливість до порушень безпеки.

Для захисту даних рекомендовано застосовувати Venafi Encryption Director, який керує ключами SSL у глобальній обчислювальній інфраструктурі, яка простягається від центру обробки даних до хмари та за її межами. Запатентовані технології, включаючи централізований портал реєстрації для всіх основних центрів сертифікації (ЦС), забезпечують просту у розгортанні функціональну сумісність, масштабованість та узгодженість між кількома типами шифрування, операційними середовищами, центрами сертифікації, HSM, додатками, каталогами та іншими корпоративними системами [9].

Інтеграція SecureSphere-Venafi Encryption Director дозволяє завантажувати ключі SSL у SecureSphere Management Server (MX).

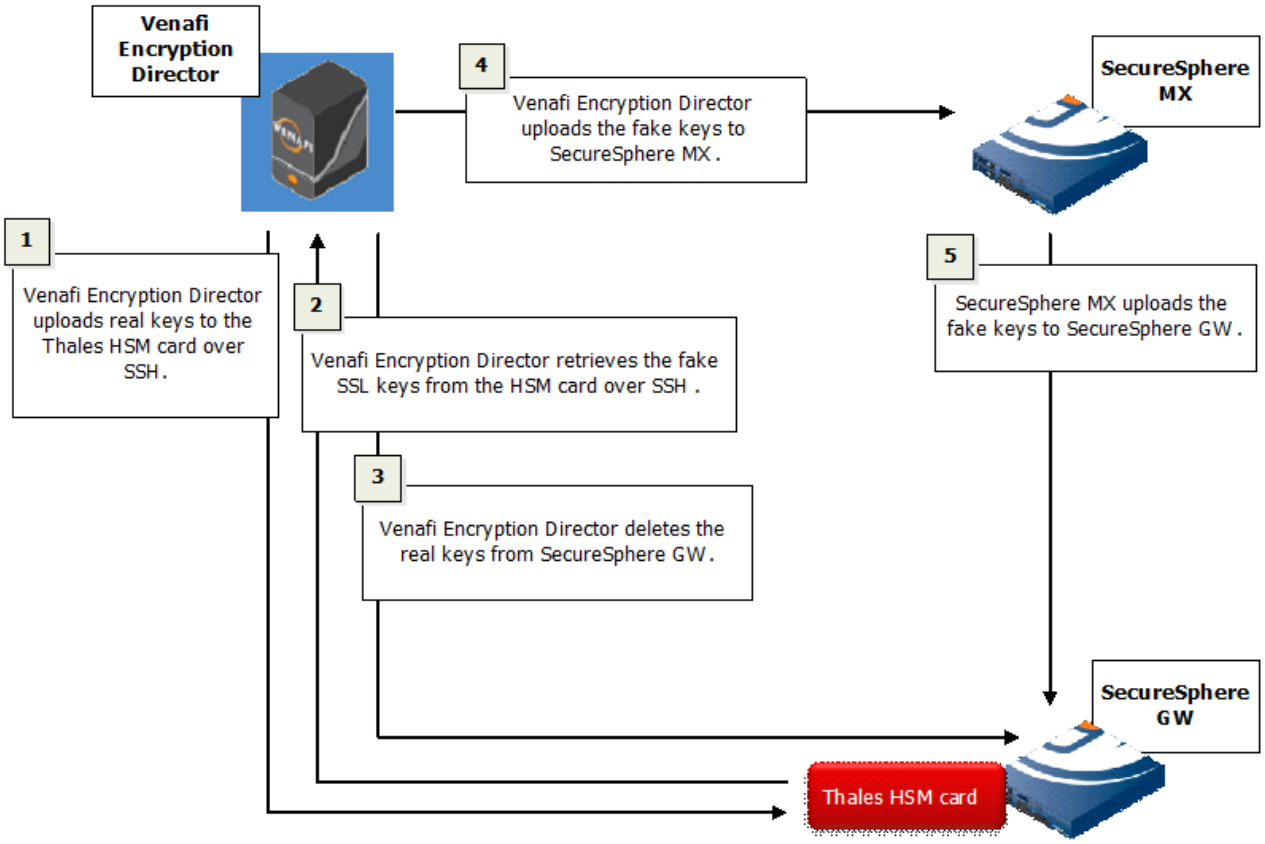

Рис.3.2. Етапи інтеграції Venafi Encryption Director [9]

Етапи інтеграції (показані на малюнку вище) полягають у наступному:

1. Venafi Encryption Director завантажує справжні ключі SSL на картку Thales HSM, встановлену на SecureSphere Gateway, через SSH.

Під час цього процесу реальні ключі SSL тимчасово перебувають у оперативній пам'яті SecureSphere Gateway. Ключі буде видалено на кроці 5.

2. Карта HSM створює підроблені ключі SSL, що відповідають реальним ключам SSL, а Venafi Encryption Director витягує підроблені ключі SSL з картки HSM.

3. Venafi Encryption Director видаляє реальні ключі SSL із SecureSphere Gateway.

На цьому етапі ці ключі SSL зберігаються лише на карті HSM.

4. Venafi Encryption Director завантажує підроблені ключі SSL у SecureSphere MX.

5. SecureSphere MX завантажує підроблені ключі SSL у SecureSphere Gateway.

SecureSphere GW потребує підроблених ключів SSL для отримання реальних ключів SSL з картки HSM при необхідності [8-9].

3.3 Налаштування агентів SecureSphere

Для роботи інфраструктури організації необхідно використовувати агентів, які будуть збирати інформацію подій від файлових серверів. Це можуть бути локальні та віртуальні агенти [10, 11].

Ви можете встановити SecureSphere Agent на віртуальну машину, розташовану в Microsoft Azure. Зверніть увагу на таке:

• Агенти SecureSphere в Azure будуть працювати з наступним розгортанням: сервери баз даних з агентом можуть бути розташовані в Azure, а сервер керування та шлюз повинні бути розташовані разом, локально або в загальнодоступній хмарі Azure.

• Установка SecureSphere Agent в Azure в усіх відношеннях ідентична будь-якій іншій установці

щоб встановити та налаштувати SecureSphere Agent (найбільш типові сценарії):

Контрольний список завдань SecureSphere Agent [10,11]:

1. Отримайте останню версію SecureSphere Agent для своєї платформи з FTP-сайту Imperva або оновлення програмного забезпечення.

Переконайтеся, що ви завантажили правильний файл установки агента для своєї платформи.

Перш ніж перейти до наступного кроку, уважно ознайомтеся з примітками до випуску.

2. Перевірте конфігурацію операційної системи бази даних або файлового сервера.

Переконайтеся, що правильна версія програмного забезпечення бази даних (включаючи виправлення), і що налаштовано правильно.

3. Налаштуйте SecureSphere Gateway. Налаштуйте шлюз так, щоб він міг взаємодіяти з SecureSphere Agent.

4. Встановіть SecureSphere Agent. Встановіть SecureSphere Agent на базу даних та/або файловий сервер.

5. Зареєструйте SecureSphere Agent на шлюзі. Зареєструйте агента на шлюзі, щоб він міг розпочати моніторинг.

6. Налаштуйте SecureSphere Agent за допомогою графічного інтерфейсу SecureSphere. Налаштуйте SecureSphere Agent у вікні «Агенти» у SecureSphere.

7. Усунення несправностей та контроль. Використовуйте консоль керування для усунення несправностей та керування.

Мониторинг активности базы данных SecureSphere Agent відбувається за рахунок того, що він встановлений на сервері бази даних. SecureSphere Agent може відстежувати всі дії з базою даних, включаючи:

• Локальна діяльність: наприклад, операції, які виконуються адміністраторами або адміністраторами баз даних, які виконуються TCP, або іншим механізмом IPC.

• Мережева активність: яка може бути видима для SecureSphere Gateway, залежно від розгортання.

Лише агенти SecureSphere можуть відстежувати активність файлів та SharePoint.

SecureSphere Agent перехоплює трафік у різний спосіб, у тому числі за допомогою завантажуваного компонента ядра. SecureSphere може блокувати трафік, що відстежується SecureSphere Agent, за допомогою правил моніторингу агента та налаштування політик безпеки для блокування трафіку.

Кожен SecureSphere Agent зареєстрований на одному або кількох шлюзах SecureSphere, на які він надсилає дані та інформацію про стан і з яких отримує

оновлення конфігурації. SecureSphere Agent є легким і накладає мінімальні накладні витрати на сервер бази даних - він виконує лише мінімальний аналіз перехопленого трафіку, перш ніж перенаправити його на шлюз. SecureSphere Agent взаємодіє зі шлюзом SecureSphere Gateway через тунель, що настроюється (SSL або не SSL).

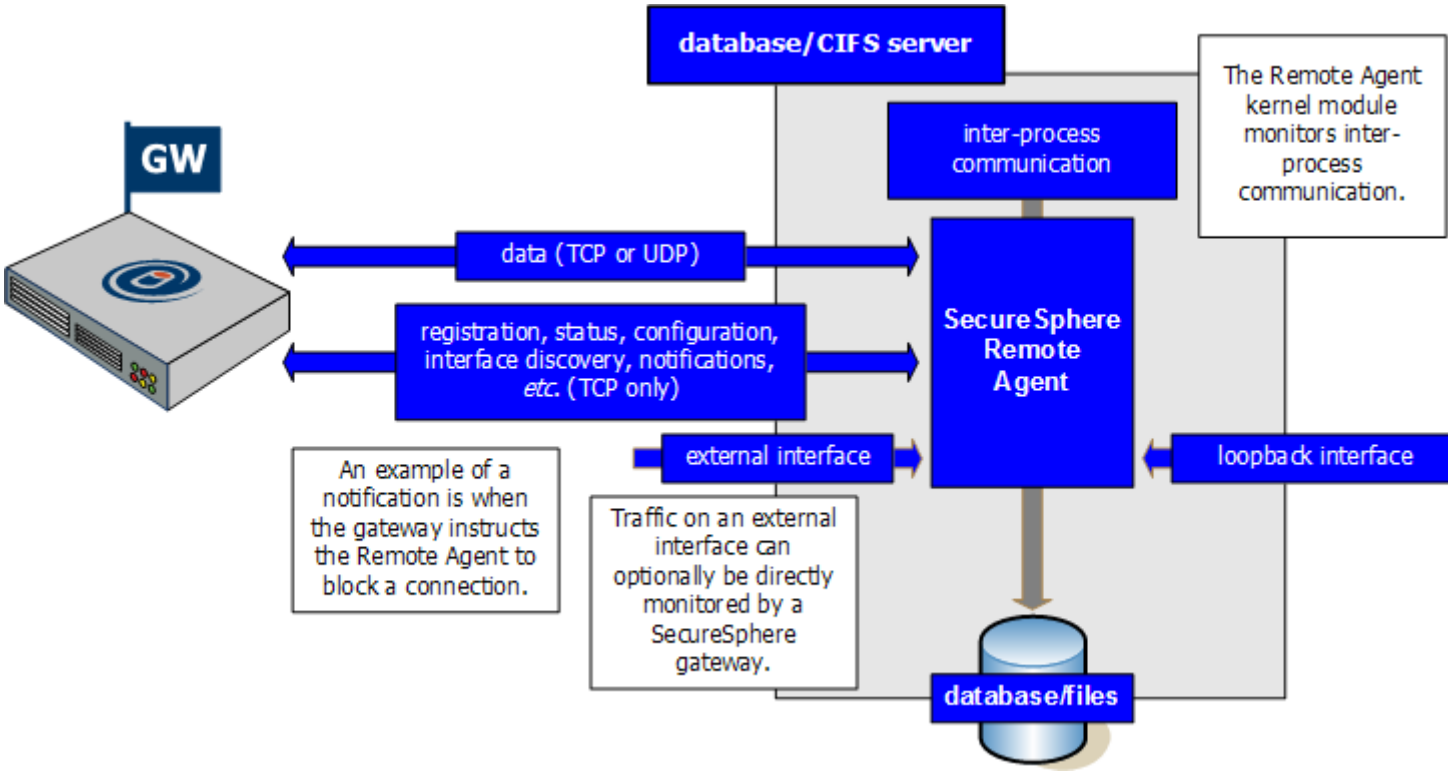

Рис. 3.3. Сценарій роботи SecureSphere Agent [10]

У типовому сценарії SecureSphere Agent надсилає локальне повідомлення на інтерфейсі керування SecureSphere Gateway через TCP-тунель, який можна налаштувати як SSL-з'єднання. Можна визначити два окремих канали: один для інформації управління та конфігурації (двонаправлений канал між агентом і шлюзом, завжди TCP) і один для даних (що надсилається тільки агентом SecureSphere на шлюз, тобто TCP).

SecureSphere Agent складається з кількох процесів [10, 11]:

• Процес SecureSphere Agent, який відстежує з'єднання з базою даних.

• Процес контролера SecureSphere Agent, який керує обміном даними між SecureSphere Gateway та SecureSphere Agent (управління, стан, конфігурація, виявлення інтерфейсів)

• Процес сторожового таймера, який примусово обмежує та перезапускає процес SecureSphere Agent у разі збою.

SecureSphere Agent відстежує ланцюжок користувачів ОС, тому, якщо локальний користувач входить до системи з одним ім'ям користувача ОС, а потім виконує серію «змін ідентичності» за допомогою команди, SecureSphere Agent буде включати ланцюжок імен користувачів. та IP-адресу віддаленого входу до контрольного запису. Крім того, IP-адреса віддаленого входу буде вказана як вихідна IP-адреса замість фіктивної IP-адреси, визначеної в розділі "Фіктивні параметри мережі" на вкладці "Установки" [10, 11]

Ланцюжок користувачів ОС доступний як критерій відповідності для використання в політиках безпеки, збагачення даних та аудиту.

У політиках аудиту критерій відповідності Source of Activity може використовуватися для вказівки вихідної IP-адреси.

На вкладці «Критерії відповідності» політики можна вказати ланцюжок користувачів ОС як критерій відповідності. Якщо ім'я обраного користувача ОС є десь у ланцюжку, збіг вважається успішним (рис.3.4).

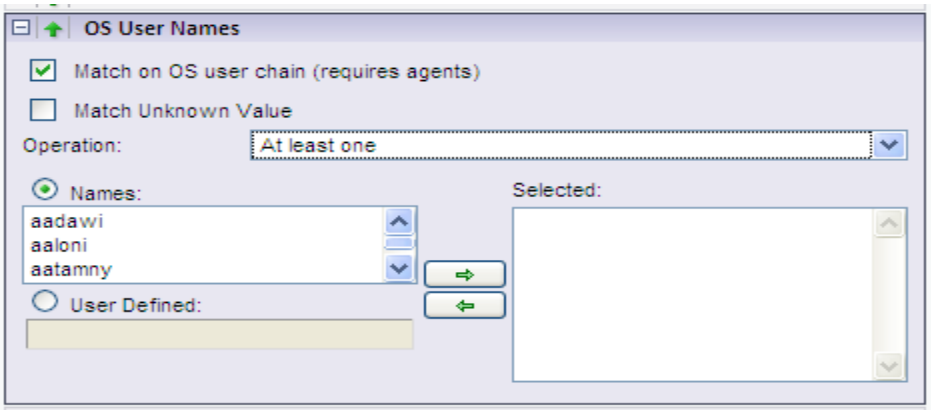

Рис. 3.4. Ланцюжок користувачів критерію відповідності [11]

Агенти SecureSphere дозволяють відстежувати зовнішній трафік одним із наступних способів [10,11]:

• EIK - External-in-Kernel: власний метод перехоплення Imperva, який використовує модуль ядра SecureSphere.

• PCAP - Packet Capture: стандартний метод перехоплення цифрового зв'язку.

Трафік, який можна відстежувати, можна розділити на два типи:

• Зовнішній трафік - коли користувачі підключаються ззовні безпосередньо до бази даних за допомогою TCP. Блокування зовнішнього трафіку підтримується на всіх платформах Unix/Linux (включаючи Solaris, AIX та HP-UX), а також на Windows 2008 та новіші.

• Внутрішній трафік - це трафік, який створюється процесом, запущеним на тому самому комп'ютері.

Якщо необхідно заблокувати зовнішній трафік за допомогою SecureSphere, SecureSphere Agent має бути налаштований на використання EIK. EIK увімкнено за замовчуванням.

3.4 Технологія Imperva WAF для забезпечення захисту від кіберзагроз

Програмне рішення Imperva WAF призначене для адаптації до загроз, усунення ризику кібератак, зменшення витоку даних та забезпечення відповідності веб-додатків нормативним вимогам, таким як PCI DSS 6.6.

Коли веб-програми зазнають атаки, служба вимикається, а конфіденційні дані можуть бути викрадені. Брандмауер веб-додатків Imperva перевіряє та аналізує вхідні запити до додатків з метою запобігання будь-яким формам кібератак. Imperva WAF - це хмарний сервіс, який захищає інфраструктуру організації від багаторівневих атак, включаючи загрози нульового дня і топ-10 OWASP.

Тож основним призначенням WAF є моніторинг, фільтрація та блокування вхідних та вихідних пакетів даних із веб-програми або веб-сайту. WAF може бути хостовими, мережевими або хмарними і зазвичай розгортаються через зворотні проксі-сервери і розміщуються перед програмою або веб-сайтом (або декількома програмами та сайтами).

WAF можуть працювати як мережні пристрої, серверні плагіни або хмарні сервіси, перевіряючи кожен пакет та аналізуючи логіку прикладного рівня (рівень 7) відповідно до правил фільтрації підозрілого або небезпечного трафіку.

Одним з таких додаткових рішень є Imperva Incapsula, яка використовується в основному в режимі блокування, оскільки вона може виключати помилкові спрацьовування через механіку, орієнтовану на додаток, та динамічне профілювання. Доступ до графічного інтерфейсу Incapsula здійснюється через онлайн-консоль керування за допомогою веб-браузера. Сервіси безпеки WAF від Imperva оснащені функціями захисту від DDoS-атак та швидким CDN.

Служба легко налаштовується, сертифікована PCI та готова до роботи з SIEM та призначена для єдиної мети – блокувати загрози з мінімальною кількістю помилкових спрацьовувань.

Переваги використання Imperva WAF

Imperva Web Application Firewall високо оцінений аналітиками та призначений для боротьби з загрозами безпеці веб-додатків. Він використовується середніми та великими організаціями для боротьби з будь-якими потенційними порушеннями безпеки.

Особливості роботи Imperva WAF

Технологія Imperva Incapsula CDN - це шлях для всього вхідного трафіку до вашого веб-додатку. Це робить його ідеальним місцем для фільтрації шкідливих запитів, таких як XSS-атаки, SQL-ін'єкції тощо. Imperva Incapsula виявляє загрози за

допомогою різних рівнів політик безпеки, які регулярно оновлюються і підтримуються командою безпеки світового класу.

WAF важливі для зростаючої кількості організацій, які пропонують продукти або послуги в Інтернеті, включаючи розробників мобільних додатків, постачальників соціальних мереж та цифрових банкірів. WAF може допомогає захистити конфіденційні дані, такі як записи клієнтів і дані платіжних карток, і запобігти їх витоку.

Організації зазвичай зберігають більшу частину своїх конфіденційних даних у серверній базі даних, до якої можна отримати доступ через веб-програми. Компанії все частіше використовують мобільні програми та пристрої IoT для полегшення бізнес-взаємодії, при цьому багато онлайн-транзакцій відбуваються на рівні додатків. Тому зловмисники часто націлені на програми, щоб отримати доступ до цих даних.

Використання WAF може допомогти вам виконати вимоги відповідності, такі як PCI DSS (стандарт безпеки даних індустрії платіжних карток), який застосовується до будь-якої організації, що обробляє дані власників карток, і вимагає встановлення брандмауера. Таким чином, WAF є важливим компонентом моделі безпеки організації.

Важливо мати WAF, але рекомендується поєднувати його з іншими заходами безпеки, такими як системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS) та традиційні брандмауери для досягнення моделі глибокоешелонованого захисту.

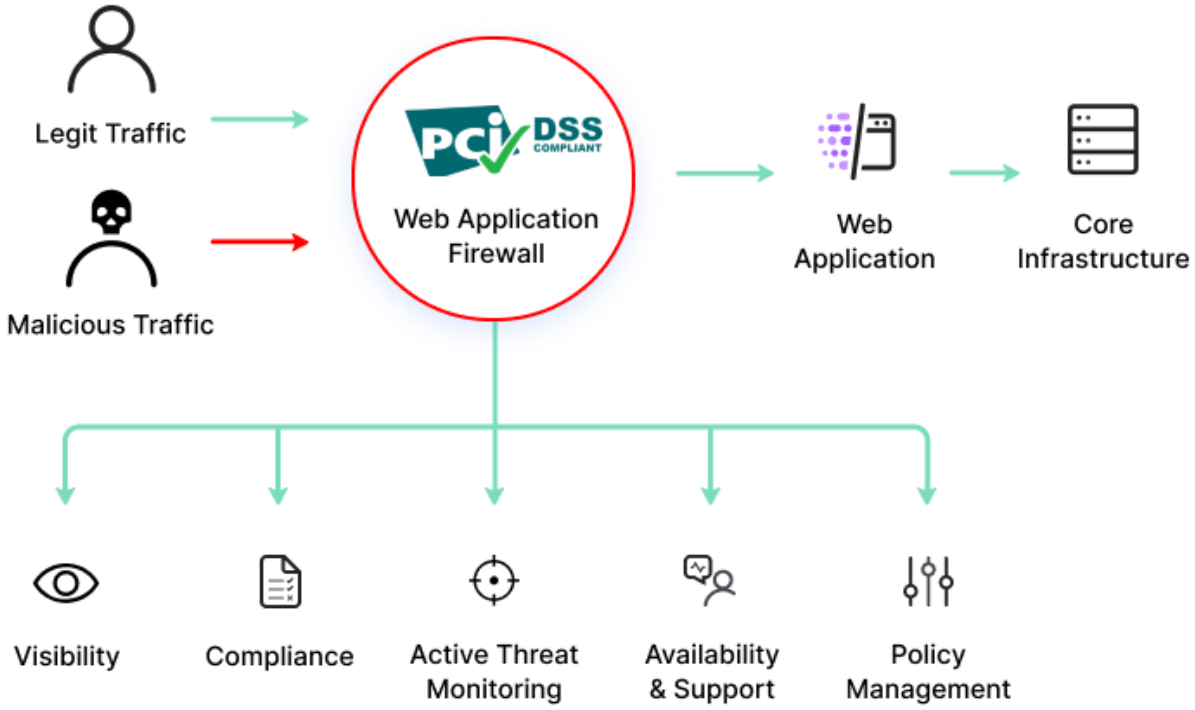

Рис. 3.5 Основні функції WAF

Визначимо типи брандмауерів веб-додатків

Є три основні способи реалізувати WAF:

• Мережевий WAF - зазвичай апаратний, він встановлюється локально, щоб зменшити затримку. Однак це найдорожчий тип WAF, що потребує зберігання та обслуговування фізичного обладнання.

• WAF на основі хоста – може бути повністю інтегрований у програмне забезпечення програми. Цей варіант дешевше, ніж мережні WAF, і більш налаштований, але він вимагає значних ресурсів локального сервера, складний у реалізації і може бути дорогим в обслуговуванні. Машину, яка використовується для запуску WAF на основі хоста, часто необхідно зміцнити та налаштувати, що може зайняти час і бути дорогим.

• Хмарний WAF – доступне, легко реалізоване рішення, яке зазвичай не потребує попередніх вкладень, при цьому користувачі оплачують щомісячну або річну передплату на послугу «Безпека як послуга». Хмарний WAF можна регулярно

оновлювати без додаткових витрат і без будь-яких зусиль користувача. Однак, оскільки ви покладаєтеся на сторонню організацію для керування своїм WAF, важливо переконатися, що хмарні WAF мають достатні параметри налаштування, щоб відповідати бізнес-правилам організації.

Архітектура WAF побудована таким чином, що створюється захищений периметр інфрастуктури організації, де забезпечується захист бази даних серверів, серверів додатків та web-сервера. Функції WAF допомогають виявляти загрози за рахунок використання інформації про атаки з своєї мережі для захисту всіх клієнтів мережі.

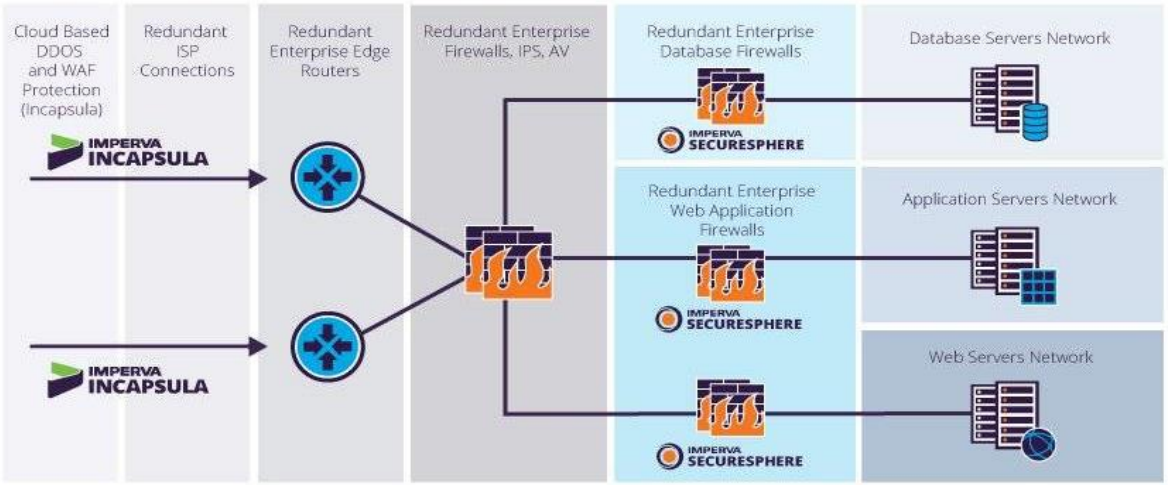

Рис. 3.6. Архітектура WAF [12]

Тож згідно архітектури визначимо основні функції та можливості WAF.

WAF зазвичай пропонують такі функції та можливості, які показано в таблиці 3.1.

Таблиця 3.1

Функції та можливості WAF

	**Базы даних сигнатур атак**	Сигнатури атак - це шаблони, які можуть вказувати на шкідливий трафік, включаючи типи запитів, аномальні відповіді сервера та відомі шкідливі IP-адреси. Раніше WAF покладалися переважно на бази даних шаблонів атак, які менш ефективні проти нових чи невідомих атак.
	**Аналіз шаблонів трафіку на базі штучного інтелекту**	Алгоритми штучного інтелекту дозволяють проводити поведінковий аналіз моделей трафіку, використовуючи базові поведінкові параметри для різних типів трафіку, щоб виявляти аномалії, що вказують на атаку. Це дозволяє виявляти атаки, які не відповідають відомим шкідливим шаблонам.
	**Профілювання додатків**	Це включає аналіз структури програми, включаючи типові запити, URL-адреси, значення і дозволені типи даних. Це дозволяє WAF виявляти та блокувати потенційно шкідливі запити.
	**Налаштування**	Оператори можуть визначати правила безпеки, які застосовуються до трафіку додатків. Це дозволяє організаціям налаштовувати поведінку WAF відповідно до своїх потреб та запобігати блокуванню легітимного трафіку.
	**Механізми кореляції**	Вони аналізують вхідний трафік і сортують його за допомогою відомих сигнатур атак, профілювання додатків, аналізу штучного інтелекту та настроюваних правил, щоб визначити, чи слід його блокувати.
	**Платформи захисту від DDoS-атак**	Ви можете інтегрувати хмарну платформу, яка захищає від розподілених атак типу «відмова в обслуговуванні» (DDoS). Якщо WAF виявляє DDoS-атаку, він може передавати трафік на платформу захисту від DDoS-атак, яка може обробляти великий обсяг атак.
	**Мережі доставки контенту (CDN)**	WAF розгортаються на межі мережі, тому хмарний WAF може надати CDN для кешування веб-сайту та скорочення часу його

		завантаження. WAF розгортає CDN у кількох точках присутності (PoP), які розподілені у всьому світі, тому користувачі обслуговуються з найближчого PoP.

Для WAF визначено наступні моделі безпеки. WAF можуть використовувати позитивну або негативну модель безпеки або їхню комбінацію:

• Модель позитивної безпеки - позитивна модель безпеки WAF включає білий список, який фільтрує трафік відповідно до списку дозволених елементів і дій - все, що немає в списку, блокується. Перевага цієї моделі в тому, що вона може блокувати нові або невідомі атаки, на які розробник не очікував.

• Модель негативної безпеки – негативна модель включає чорний список (або список заборон), який блокує лише певні елементи – все, що не входить до списку, дозволено. Цю модель простіше реалізувати, але вона не може гарантувати, що всі загрози будуть усунені. Це також вимагає ведення потенційно довгого списку шкідливих сигнатур. Рівень безпеки залежить від кількості введених обмежень.

Тож для захисту інфраструктури організації WAF з Imperva надає певні переваги та позитивні моменти.

Imperva надає найкращий в галузі брандмауер веб-додатків, який запобігає атакам за допомогою аналізу веб-трафіку ваших додатків світового класу.

Крім WAF, Imperva забезпечує комплексний захист додатків, API та мікросервісів:

Самозахист програм під час виконання (RASP). Виявлення та запобігання атакам у реальному часі з середовища виконання додатків завжди під рукою. Зупиніть зовнішні атаки та ін'єкції та скоротите кількість накопичених уразливостей.

Безпека API - Автоматичний захист API забезпечує захист кінцевих точок API у міру їх публікації, захищаючи ваші програми від експлуатації.

Розширений захист від ботів - запобігання атакам на бізнес-логіку з усіх точок доступу - веб-сайтів, мобільних додатків та API. Отримайте прозору видимість та контроль над трафіком ботів, щоб зупинити онлайн-шахрайство шляхом захоплення облікового запису або збору конкурентних цін.

Захист від DDoS-атак – блокуйте трафік атак на периферії, щоб забезпечити безперервність бізнесу з гарантованим часом безвідмовної роботи та без зниження продуктивності. Захистіть свої локальні або хмарні ресурси - незалежно від того, чи розміщені ви в AWS, Microsoft Azure або Google Public Cloud.

Аналітика атак - забезпечує повну видимість за допомогою машинного навчання та досвіду в предметній області всього стеку безпеки додатків, щоб виявляти закономірності в шумі та виявляти атаки додатків, що дозволяє ізолювати та запобігати кампанії атак.

Захист на стороні клієнта. Забезпечте прозорість та контроль над стороннім кодом JavaScript, щоб знизити ризик шахрайства в ланцюжку поставок, запобігти витоку даних та атакам на стороні клієнта.

Особливості даної технології полягає в наступному.

WAF може бути вбудований в програмні плагіни на стороні сервера або апаратні пристрої, або вони можуть бути запропоновані як служба фільтрації трафіку. WAF можуть захищати веб-програми від шкідливих або зламаних кінцевих точок та функціонувати як зворотні проксі-сервери (на відміну від проксі-сервера, який захищає користувачів від шкідливих веб-сайтів).

WAF забезпечують безпеку, перехоплюючи та досліджуючи кожен HTTP-запит. Незаконний трафік можна перевірити за допомогою різних методів, таких як відбитки пальців, аналіз введення CAPTCHA , і якщо вони здаються незаконними, їх можна заблокувати.

У WAF попередньо завантажені правила безпеки, які можуть виявляти та блокувати багато відомих шаблонів атак - зазвичай до них відносяться основні

вразливості безпеки веб-додатків, що підтримуються Open Web Application Security Project (OWASP).

Крім того, організація може визначати власні правила та політики безпеки відповідно до бізнес-логіки свого додатка. Для налаштування та налаштування WAF можуть знадобитися спеціальні знання.

Отже, зробимо висновок Imperva WAF захищє від нещодавно виявлених уразливостей має важливе значення у глобальному кіберсередовищі, яке постійно бореться з новими атаками, винайденими кіберзлочинцями. Крім того, служба Imperva WAF усуває перешкоди ваших веб-додатків та підвищує продуктивність файлових серверів інфраструктури організації.

ВИСНОВКИ

В інфраструктурі будь-якої організації використовуються серверне обладнання для ефективного виконання бізнес-процесів. Тому велику увагу приділяється щодо захисту їх від атак, які можуть зупинити роботу всієї організації.

В результаті виконання магістерської роботи при виконанні поставлених наукових задач, було отримано наступні результати.

Використання файлових серверів спрощує процес виконання спільної роботи з документацією та базами даних. Я перевага використання файлового сервера усуває ресурсні обмеження для користувачів і надає низку переваг, які дозволяють підвищити рівень безпеки роботи в інформацією, яка на них зберігається.

В результаті проведеного аналізу кількості атак на інформаційні системи організацій, було встановлено, що за останній час кількість атак суттєво знизилось. Це пов’язано з тим, що компанії вже встигли адаптуватись до роботи в умовах пандемії і підготували свої інформаційні системи до віддаленого доступу. Але це в свою чергу, не виключає, що атаки на інфраструктуру припиняться. Аналіз показав, що основні наміри зловмисників – отримання даних (конфіденційна та персональна інформація) та фінансова вигода. Ці атаки найбільш проходять через електронну пошту або компроментацію серверів та мережевого обладнання.

Для забезпечення безпеки серверів організації в результаті порівняння було вибрано рішення Imperva Imperva SecureSphere File Security, здійснюють безперервний моніторинг та аудит усіх операцій із файлами в реальному часі без зниження продуктивності та доступності файлових серверів.

Рішення SecureSphere File Security надають захист конфіденційних файлів на файлових серверах, пристроях зберігання та репозиторіях.

В результаті дослідження було встановлено, що архітектура системи SecureSphere складається з шлюзу моніторингу та безпеки та серверу керування. Тож надалі було запропоновано варіант технології безпеки інфраструктури організації на

базі рішення SecureSphere. Для обраного варіанту було досліджено функції кожного з компонентів, які представлено у вигляді рекомендацій для фахівців з кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Предназначение и функции файлового сервера [електронний ресурс] режим доступу: https://www.0552.ua/list/318013

2. Призначення, створення та установка сервера [електронний ресурс] режим доступу: https://www.key4.com.ua/ustanovka-i-nastrojka-serverov/

3. 2. Функції файлового сересеру [електронний ресурс] режим доступу: https://itelon.ru/blog/faylovyy-server/

4. v12.6 Guide File Security [електронний ресурс] режим доступу: https://docs.imperva.com/bundle/v12.6-file-security-user-guide/page/375.htm .

5. Актуальні кіберзагрози: II квартал 2021 року [електронний ресурс] режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/.

6. 10 способів захистити файловий сервер [електронний ресурс] режим доступу: https://www.lepide.com/blog/top-10-ways-to-secure-your-file-servers/amp/

7. [електронний ресурс] режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/

8. MX сервер [електронний ресурс] режим доступу: https://docs.imperva.com/bundle/v14.5-dam-administration-guide/page/8582.htm

9. NIST. publication/1800-16 Securing Web Transactions. TLS Server Certificate, Management. 2020 [електронний ресурс] режим доступу: https://www.nccoe.nist.gov/publication/1800-16/VolC/index.html

10. SecureSphere Agent [електронний ресурс] режим доступу: https://docs.imperva.com/bundle/v14.5-dam-administration-guide/page/7325.htm

11. Налаштування SecureSphere Agent [електронний ресурс] режим доступу: https://docs.imperva.com/bundle/v14.5-dam-administration-guide/page/7324.htm .

12. Web-Application-Firewall [електронний ресурс] режим доступу: https://www.dataguardstore.com/Web-Application-Firewall.asp

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)