ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

Дослідження шляхів та розробка рекомендацій щодо захисту від шкідливих програм корпоративного середовища на базі Acronis

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та
кібернетична безпека»
(шифр і назва спеціальності)
Кисільова Д.В.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

РЕФЕРАТ

Текстова частина бакалаврської роботи: 60 сторінок, 13 рисунків, 10 джерел.

Об’єкт дослідження – процес захисту від шкідливих програм корпоративного середовища організації.

Предмет дослідження – методи та засоби захисту від шкідливих програм корпоративного середовища організації на базі Acronis.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту від шкідливих програм корпоративного середовища організації на базі Acronis.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Робота присвячена дослідженню шляхів та розроблення рекомендацій щодо захисту корпоративного середовища від шкідливих програм. В роботі проведенно аналіз поняття корпоративного середовища, його види. Отриманодані щодо впливу шкідливих програм на діяльність організацій. Проведено порівняльний аналіз різних рішень захисту від шкідливих програм, на основі якого будл досліджено архітектуру, функції рішення Acronis Cyber Protect. В результаті роботи було надані рекомендації щодо роботи модуля виявлення шкідливих програм Acronis Cyber Protect та загальні рекомендації щодо захисту корпоративного середовища від шкідливих програм.

Галузь використання – кібербезпека корпоративних інформаційних систем.

КОРПОРАТИВНЕ СЕРЕДОВИЩЕ, ЗАГРОЗИ, КІБЕРБЕЗПЕКА, ЗАХИСТ ДАНИХ, КОНФІЕНЦІЙНІСТЬ, ШКІДЛИВІ ПРОГРАМИ, , МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

TCP - Transmission Control Protocol

DNS - Domain Name System

HTTP - HyperText Transfer Protocol

ПЗ – програмне забезпечення

DGA - алгоритми генерації домену

API -application Programming Interface

NIST - National Institute of Standards and Technology

SSL/TLS - ecure Sockets Layer/ Transport Layer Security

Protect – захист

Ransomware – програма-вимагач

ВСТУП

Актуальність дослідження. Виявлення шкідливих програм в організаціях має важливе значення для забезпечення безпеки систем і даних. Шкідливі програми, такі як віруси, хробаки, трояни та програми-вимагачі, можуть завдати значної шкоди IT-інфраструктурі організації та порушити бізнес-операції. Основні причини впровадження засобів виявлення шкідливих програм в організаціях полягає у ранньому їх виявленні, має вирішальне значення для мінімізації шкоди, спричиненої кібератакою. Раннє виявлення може допомогти запобігти поширенню зловмисного програмного забезпечення на інші системи, обмежити масштаб атаки та зменшити кількість втрачених або викрадених даних.

Захист конфіденційних даних забезпечить від викрадення конфіденційних даних, наприклад інформацію про клієнтів, фінансові дані та інтелектуальну власність. Виявлення та блокування цих програм може допомогти запобігти витоку даних і захистити репутацію організації.

У багатьох галузях є нормативні вимоги, які вимагають виявлення та запобігання кібератакам. Наявність засобів виявлення зловмисних програм може допомогти організаціям виконати ці вимоги відповідності та уникнути покарань.

Виявлення шкідливих програм також є важливим для реагування на інциденти. Коли відбувається кібератака, організації повинні мати можливість швидко визначити джерело атаки та вжити відповідних заходів для зменшення збитку. Для цього потрібні ефективні засоби виявлення та аналізу шкідливих програм.

Тож, наявність засобів виявлення шкідливих програм в організаціях має вирішальне значення для забезпечення безпеки систем і даних. Завдяки ефективним інструментам і процесам виявлення організації можуть зменшити ризик кібератак, захистити конфіденційні дані, відповідати нормативним вимогам і швидко реагувати на інциденти безпеки. Таким чином, виявлення програм-вимагачів в інфраструктурі організації має вирішальне значення для запобігання та пом’якшення впливу атак програм-вимагачів, які можуть мати серйозні наслідки

для організацій будь-якого розміру. Тому тема бакалаврської роботи є своєчасною та актуальною.

Об'єкт дослідження – процес захисту від шкідливих програм корпоративного середовища організації.

Предмет дослідження – розробити рекомендації щодо застосування методів та засобів захисту від шкідливих програм корпоративного середовища організації на базі Acronis.

Мета роботи – розробити рекомендації щодо застосування методів та засобів від шкідливих програм корпоративного середовища організації на базі Acronis.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Завдання бакалаврської роботи:

дослідити загрози, які виникають внаслідок атак шкідливих програм;

дослідити методи та засоби захисту від шкідливих програм корпоративного середовища на базі Acronis;

розробити рекомендації щодо захисту від шкідливих програм корпоративного середовища на базі Acronis.

Практичне значення одержаних результатів: рекомендації захисту від шкідливих програм корпоративного середовища на базі Acronis можуть бути використані у сфері забезпечення кібербезпеки у корпоративних інформаційних системах.

1 АНАЛІЗ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ КОРПОРАТИВНОГО СЕРЕДОВИЩА ОРГАНІЗАЦІЙ

1.1. Аналіз корпоративного середовища організації

Корпоративне середовище — це організаційна структура, система якої визначає, як певна діяльність спрямована на досягнення цілей організації. Ці дії можуть включати правила, ролі та обов'язки. Тож надалі розглянемо організаційну структуру корпоративного середовища [1].

Організаційна структура визначає, як інформація перетікає між рівнями всередині компанії. Наприклад, у централізованій структурі рішення приймаються зверху вниз, тоді як у децентралізованій структурі повноваження щодо прийняття рішень розподіляються між різними рівнями організації. Наявність організаційної структури дозволяє компаніям залишатися ефективними та зосередженими.

Основні положення організації корпоративного середовища полягають у наступному [1]:

1. організаційна структура визначає, як певна діяльність спрямована на досягнення цілей організації.

2. успішні організаційні структури визначають роботу кожного працівника та те, як вона вписується в загальну систему.

3. централізована структура має визначений ланцюг командування, тоді як децентралізовані структури дають майже кожному працівнику високий рівень особистої відповідальності.

4. типи організаційних структур включають функціональні, дивізіональні, плоскі і матричні структури.

Керівники вищої ланки повинні розглянути низку факторів, перш ніж вирішити, який тип організації найкращий для їхнього бізнесу, включаючи бізнес-цілі, галузь і культуру компанії.

Розуміння організаційної структури. Підприємства будь-яких форм і розмірів активно використовують організаційні структури. Вони визначають певну ієрархію всередині організації. Успішна організаційна структура визначає роботу кожного працівника та те, як вона вписується в загальну систему. Простіше кажучи, організаційна структура визначає, хто що робить, щоб компанія могла досягти своїх цілей[1].

Таке структурування дає компанії візуальне уявлення про те, як вона сформована та як їй найкраще просуватися вперед у досягненні своїх цілей. Організаційні структури зазвичай зображені на певній діаграмі або схемі, як-от піраміда, де найвпливовіші члени організації сидять на вершині, а ті, що мають найменшу владу, знаходяться внизу.

Відсутність офіційної структури може виявитися складним для певних організацій. Наприклад, співробітникам може бути важко зрозуміти, перед ким вони повинні звітувати. Це може призвести до невизначеності щодо того, хто за що відповідає в організації.

Наявність структури може підвищити ефективність і забезпечити ясність для всіх на кожному рівні. Це також означає, що кожен відділ може бути більш продуктивним, оскільки він, швидше за все, буде більше зосереджений на енергії та часі.

Централізовані проти децентралізованих організаційних структур

Організаційна структура буває централізованою або децентралізованою. Традиційно організації були структуровані з централізованим керівництвом і визначеним ланцюгом командування. Військові — це організація, відома своєю високоцентралізованою структурою з довгою та специфічною ієрархією начальників і підлеглих. У централізованій організаційній системі є дуже чіткі обов’язки для

кожної ролі, при цьому підлеглі ролі за замовчуванням виконують вказівки своїх керівників[1].

Відбулося зростання кількості децентралізованих організацій, як і багатьох технологічних стартапів . Це дозволяє компаніям залишатися швидкими, гнучкими та гнучкими, оскільки майже кожен співробітник отримує високий рівень особистої відповідальності. Наприклад, Johnson & Johnson — це компанія, яка відома своєю децентралізованою структурою.

Будучи великою компанією з понад 200 підрозділами та брендами, які іноді працюють у дуже різних галузях, кожна з них працює автономно. Навіть у децентралізованих компаніях зазвичай існують вбудовані ієрархії (наприклад, операційний директор працює на вищому рівні, ніж колега початкового рівня). Однак команди мають право приймати власні рішення та дійти найкращих висновків, не обов'язково отримуючи «схвалення» згори.

Розглянемо типи організаційних структур.

Функціональна структура

У реальному світі реалізовано чотири типи загальних організаційних структур. Перший і найпоширеніший — функціональна структура. Це також називають бюрократичною організаційною структурою , яка розбиває компанію на основі спеціалізації її робочої сили. Більшість малих і середніх підприємств реалізують функціональну структуру. Поділ фірми на відділи, що складаються з маркетингу, продажів і операцій, є актом використання бюрократичної організаційної структури [1].

Дивізіональна або мультидивізіональна структура

Другий тип поширений серед великих компаній з великою кількістю бізнес-підрозділів. Компанія, яка використовує цей метод, називається дивізіональною або мультидивізіональною структурою (M-Form), структурує свою команду керівництва на основі продуктів, проектів або дочірніх компаній, якими вони керують. Хорошим прикладом такої структури є Johnson & Johnson. Маючи тисячі продуктів і напрямків

діяльності, компанія структурується таким чином, що кожен підрозділ працює як окрема компанія зі своїм президентом.

Окрім спеціалізації, підрозділи також можуть бути визначені географічно. Наприклад, глобальна корпорація може мати північноамериканський підрозділ і європейський підрозділ [1].

Командний

Подібно до підрозділів або функціональних структур, командні організації поділяються на згуртовані групи співробітників, які служать певним цілям і функціям, але де кожна команда є одиницею, яка містить як лідерів, так і працівників.

Плоска (флатархія) структура

Флатархія, також відома як горизонтальна структура, відносно нова і використовується серед багатьох стартапів. Як випливає з назви, він вирівнює ієрархію та ланцюг командування та надає своїм співробітникам велику автономію. Компанії, які використовують цей тип структури, мають високу швидкість впровадження.

Матрична структура

Фірми також можуть мати матричну структуру. Він також найбільш заплутаний і найменш використовуваний. У цій структурі розподіляються співробітники з різними керівниками, відділами або департаментами. Наприклад, працівник, який працює в матричній компанії, може мати обов’язки як у відділі продажів, так і в обслуговуванні клієнтів [1].

Кругова структура

Кругові структури є ієрархічними, але їх називають круговими, оскільки вони розміщують співробітників і менеджерів вищого рівня в центрі організації з концентричними кільцями, що розширюються назовні, і містять співробітників і персонал нижчого рівня. Цей спосіб організації призначений для заохочення відкритого спілкування та співпраці між різними рангами.

Структура мережі

Структура мережі організовує підрядників і сторонніх постачальників для виконання певних ключових функцій. Він має відносно невелику штаб-квартиру з географічно розпорошеними супутниковими офісами, а також ключові функції, передані іншим фірмам і консультантам [1].

Переваги організаційних структур

Створення організаційної структури може бути дуже корисним для компанії. Структура не тільки визначає ієрархію компанії, але й дозволяє фірмі розробити структуру оплати праці для своїх співробітників. Встановлюючи організаційну структуру, фірма може визначити рівні та діапазони зарплати для кожної посади.

Така структура також робить операції більш ефективними та ефективнішими. Розділивши співробітників і функції на різні відділи, компанія може безперешкодно виконувати різні операції одночасно [1].

Крім того, дуже чітка організаційна структура інформує працівників про те, як найкраще виконувати свою роботу. Наприклад, в ієрархічній організації співробітникам доведеться більше працювати, щоб купити прихильність або залицятися до тих, хто має повноваження приймати рішення. У децентралізованій організації співробітники повинні проявляти більше ініціативи та творчо вирішувати проблеми. Це також може допомогти встановити очікування щодо того, як працівники можуть відстежувати свій власний розвиток у компанії та підкреслювати певний набір навичок, а також для потенційних працівників, щоб оцінити, чи така компанія буде добре відповідати їхнім власним інтересам і стилям роботи.

Незалежно від того, як працює корпоративне середовище, для обміну даними і отримання відповідних сервісів клієнтам організації необхідно створити клієнт-серверну архітектуру. Тому надалі розглянемо як це повинно працювати.

В архітектурі клієнт-сервер кожен процес або комп’ютер у мережі функціонує як сервер або клієнт. Клієнтські сервери — це потужні комп’ютери, єдине призначення яких — обробка принтерів, дисків і мережевого трафіку. Клієнти

запускають свої програми на своїх робочих станціях або персональних комп'ютерах. Сервери в першу чергу забезпечують ресурси, такі як пристрої, файли та потужність обробки.

Але перш ніж краще зрозуміти архітектуру клієнт-сервер, визначимо, що таке клієнт і сервер.

Клієнт – клієнтом може бути будь-який комп'ютер, який запитує щось у сервера. Наприклад , відвідуючи будь-який веб-сайт, ми запитуємо веб-сторінку з його домену. Тому тут ми виступаємо в ролі клієнта.

Сервер – з іншого боку, сервер – це комп'ютер, призначений для обслуговування запитів клієнта. У тому ж прикладі, що й вище, клієнт запитує веб-сторінку, а потім сервер відповідає веб-сторінкою клієнту.

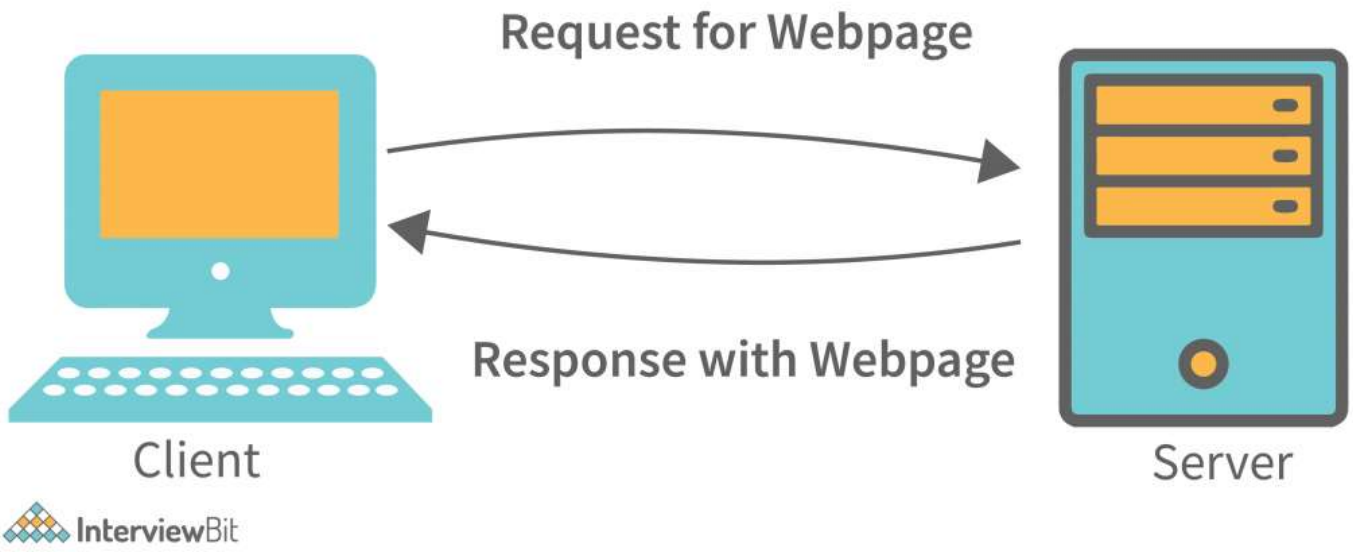


Рис.1.1. Робота клієнта і сервера [2]

Клієнт-серверна архітектура або модель — це мережа додатків, що розділяє завдання між клієнтами та серверами, які або знаходяться в одній системі, або мають спілкуватися через мережу. Щоб отримати доступ до служби, що надається сервером, сервер-клієнт надсилає запит іншій програмі, яка запускає кілька програм, які розподіляють роботу між клієнтами та діляться з ними ресурсами.

Відносини клієнт-сервер відповідають шаблону запит-відповідь і мають відповідати стандартному протоколу зв’язку, який визначає мову та правила, що використовуються для зв’язку. Зв'язок клієнт-сервер відповідає набору протоколів TCP.

Повідомлення клієнт/сервер обмінюються через протокол TCP до встановлення з’єднання. Протокол TCP визначає, як дані повинні розподілятися в пакетах, які будуть доставлятися мережами, передає пакети в мережі та приймає пакети з мереж, а також керує потоком або повторною передачею спотворених і відкинутих пакетів.

Інтернет-протокол — це протокол без з’єднання, що означає, що кожен пакет, який передається в Інтернеті, є незалежною частиною даних, не пов’язаною з жодним іншим пакетом.

Розглянемо, як працює ця архітектура.

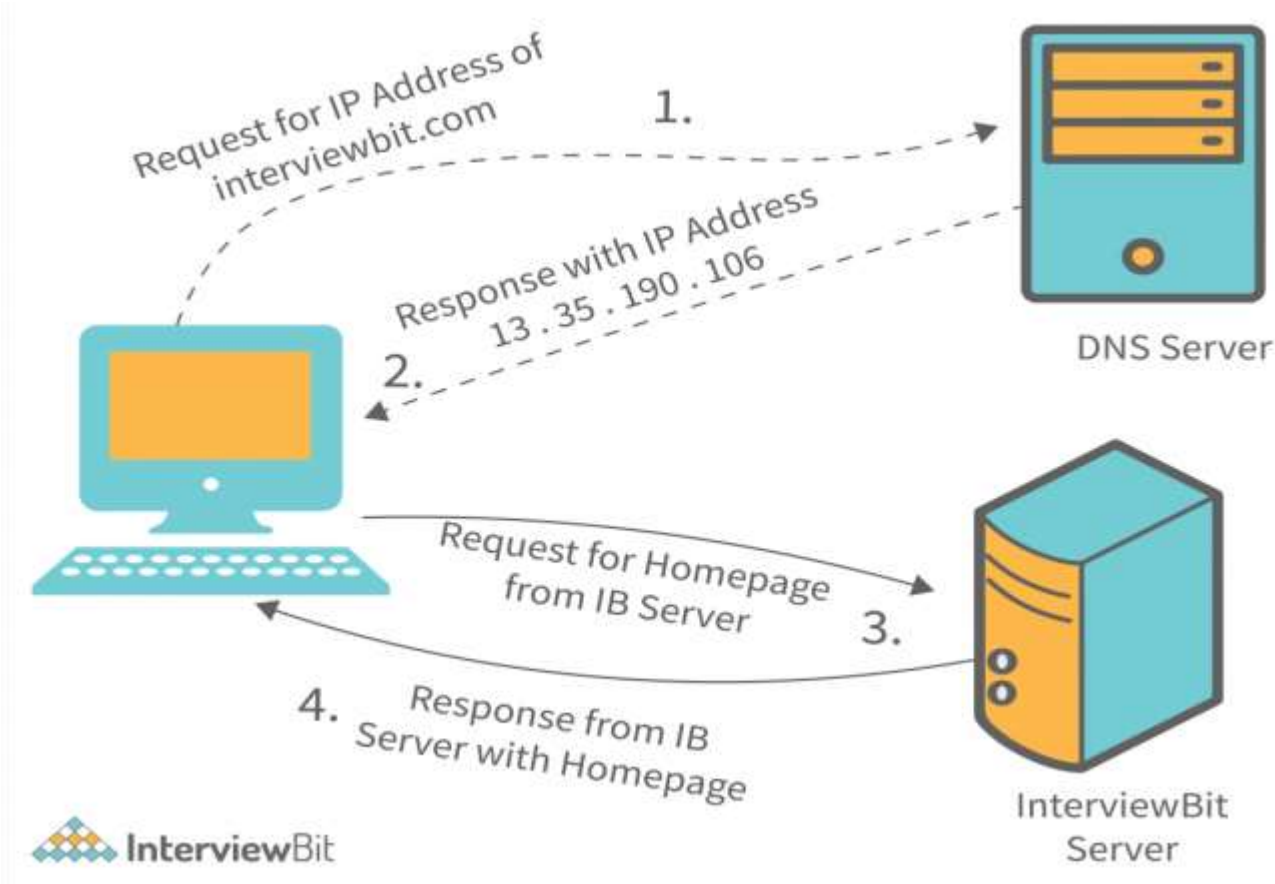


Рис.1.2. Особливості роботи клієнт-серверної архітектури [2]

На наведеному рис.1.2, якщо будь-якому клієнту потрібні дані з будь-яким сервером, він спочатку запитує IP-адресу для конкретного сервера з DNS (системи доменних імен). DNS-сервер відповідає IP-адресою. За цією IP-адресою клієнт надсилає запит на певний сервер із номером порту, указаним для конкретної програми, а потім сервер відповідає. Відповідне повідомлення отримує клієнт, і на основі номера порту пакет відповіді споживається програмою, якій він належить. Тут на дуже високому рівні зв'язок між клієнтом і сервером відбувається через HTTP-пакети.

Типи клієнт-серверної архітектури

Архітектура клієнт-сервер класифікується на різні типи на основі бізнес-логіки, реалізованої для запиту, що обробляється між клієнтом і сервером. Існують різні типи прикладів клієнт-серверної архітектури.

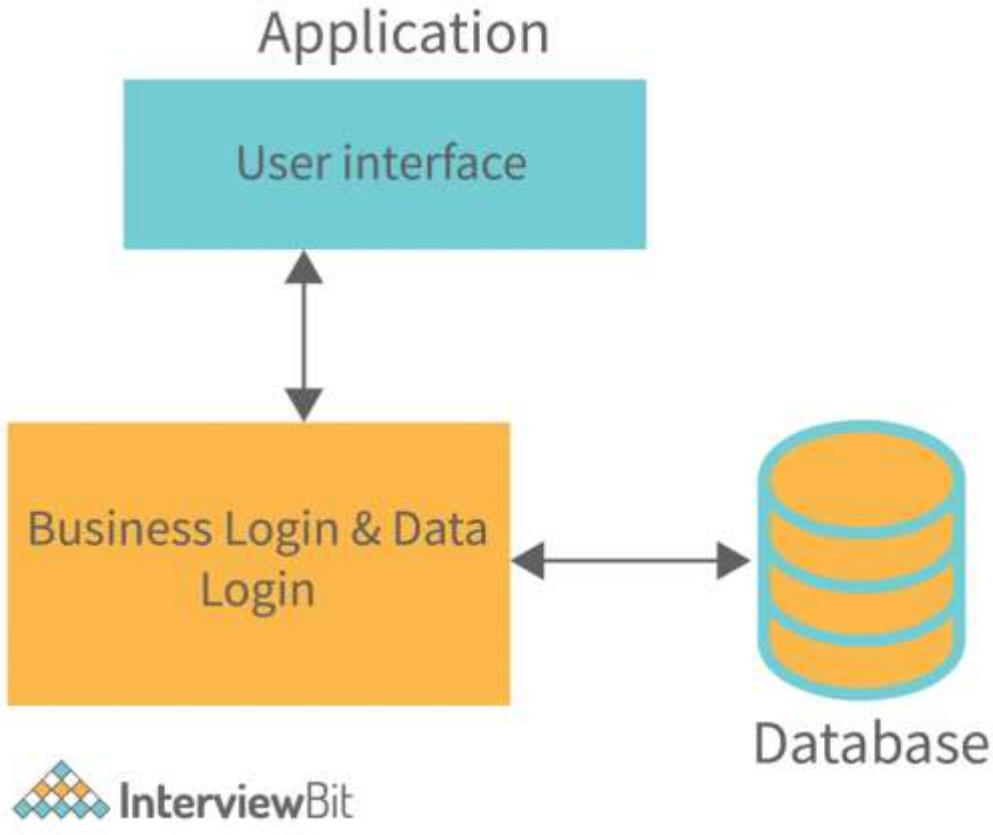


Рис.1.3. 1-рівнева архітектура [2]

У однорівневій клієнт-серверній архітектурі все, що стосується програми, групується та використовується як єдиний пакет для доставки програми. Уся логіка, пов’язана з інтерфейсом користувача, бізнес-логікою, логікою бази даних і базою даних, згрупована в одну сутність. Однорівнева архітектура пропонує різні служби, які роблять її надійним джерелом, але нею складно керувати. Розбіжність даних є основною проблемою. Робота часто дублюється. Однорівнева архітектура включає в себе кілька рівнів, включаючи презентаційний рівень, бізнес-рівень і рівень даних, які об’єднані за допомогою унікального програмного пакета. Цей рівень зазвичай зберігає дані в локальних системах або на спільному диску.

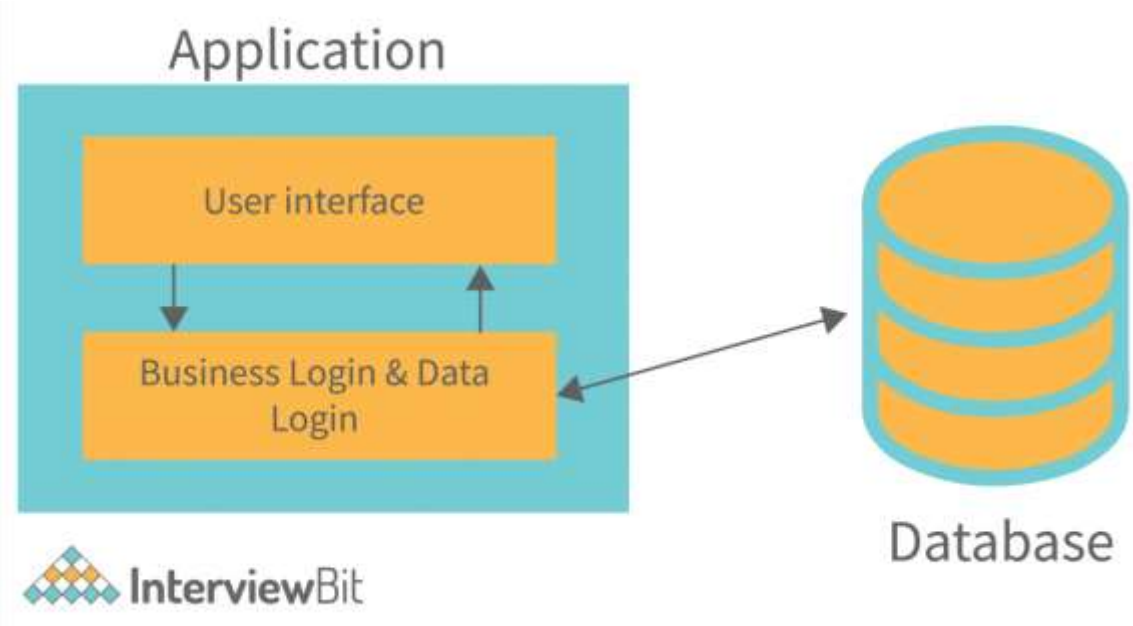


Рис.1.4. 2-рівнева архітектура [2]

У 2-рівневій клієнт-серверній архітектурі вся логіка програми розділена на 2 рівні. Основна база даних діє як окрема сутність у цій архітектурі. Бази даних розробляються окремо, а основна програма має всю логіку, пов’язану з інтерфейсом користувача, а також бізнес-логіку та логіку бази даних для зв’язку з базою даних і обробки програм. Ця архітектура має краще середовище, ніж однорівнева архітектура.

У порівнянні з однорівневими архітектурами дворівневі архітектури є швидшими, оскільки між клієнтом і сервером немає посередника. 2-рівнева

архітектура допомагає уникнути плутанини клієнта. Система онлайн-бронювання є популярним прикладом 2-рівневої архітектури.

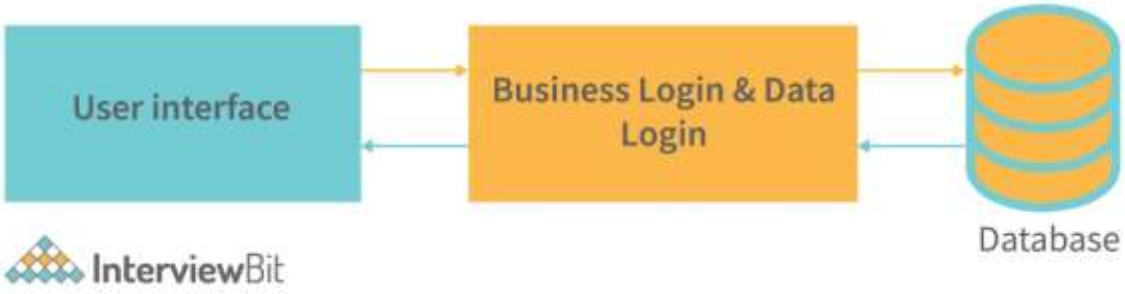


Рис.1.5. 3-рівнева архітектура [2]

На відміну від архітектури 2-рівневої системи, яка не має проміжного програмного забезпечення, 3-рівнева система має проміжне програмне забезпечення між клієнтом і сервером. Коли клієнт запитує інформацію від сервера, запит спочатку отримує проміжне програмне забезпечення. Потім запит буде надіслано на сервер для обробки. Так само сервер надішле відповідь клієнту.

У 3-рівневій архітектурі є три основні рівні: презентаційний рівень, прикладний рівень і рівень бази даних. Різні кінці кожного шару контролюють один одного. Клієнтські пристрої контролюють рівень презентації, тоді як проміжне програмне забезпечення та сервер контролюють рівень додатків і рівень бази даних відповідно. Наявність третього рівня, який забезпечує контроль даних, робить 3-рівневу архітектуру більш безпечною, має невидимі структури бази даних і забезпечує цілісність даних.

Переваги клієнт-серверної архітектури

1. **Керувати легко –** керувати файлами досить легко, оскільки всі вони зберігаються на одному сервері. Мережі клієнт-сервер мають найкраще керування для відстеження та пошуку записів необхідних файлів.

2. **Легкий доступ –** клієнти можуть входити в систему незалежно від свого місцезнаходження чи вибраної платформи, що дозволяє кожному співробітнику

отримувати доступ до своєї корпоративної інформації без використання режиму терміналу чи процесора.

3. **Сервери масштабовані –** клієнт-серверна мережа має високу масштабованість. Щоразу, коли користувач потребує, він може додати більше ресурсів, таких як клієнти та сервери, таким чином збільшуючи розмір сервера без будь-яких перерв. Через те, що сервер є централізованим, дозвіл на доступ до мережевих ресурсів не є проблемою, тому для конфігурацій потрібно дуже мало співробітників, навіть якщо розмір збільшується.

4. **Централізоване керування –** мережі клієнт-сервер мають перевагу централізованого керування, оскільки вся інформація зберігається в одному місці. Оскільки адміністратор мережі має повний контроль над керуванням і адмініструванням, це особливо корисно. У результаті будь-які проблеми, які виникають у всій мережі, можна вирішувати з одного централізованого місця. У результаті оновлювати дані та ресурси стало набагато легше.

5. **Безпека.** Завдяки централізованій архітектурі клієнт-серверні мережі добре захищають дані. Одну резервну копію можна використати для відновлення всіх файлів у разі втрати даних, наприклад, нав'язування облікових даних, таких як ім'я користувача та паролі. Інший метод забезпечення контролю доступу полягає в нав'язуванні облікових даних, таких як ім'я користувача та пароль.

Недоліки клієнт-серверної архітектури

1. **Менш надійний –** через централізовану природу клієнт-серверних мереж у разі збою або перешкод на головному сервері робота всієї мережі буде перервана. Таким чином, клієнт-серверні мережі менш надійні.

2. **Потрібне регулярне технічне обслуговування –** сервери працюватимуть у мережі безперервно. Це означає, що їх потрібно належним чином обслуговувати. Якщо є якісь проблеми, їх потрібно негайно усувати. Менеджер мережі повинен бути призначений для обслуговування сервера.

3. **Вимагає витрат –** у мережі клієнт-сервер вартість налаштування та обслуговування сервера зазвичай дуже висока, як і мережеві операції. Оскільки мережі потужні, їх придбання може бути дорогим. Таким чином, не всі користувачі зможуть ними скористатися.

4. **Перевантаженість мережі.** Якщо надто багато клієнтів звертаються до одного сервера, це може призвести до збоїв або уповільнення з'єднання. Перевантажений сервер створює багато проблем при доступі до інформації.

Архітектура клієнт-сервер дозволяє оновлювати спільну базу даних від кількох користувачів через графічний інтерфейс користувача. Усі компанії, великі чи малі, використовують потужність мережевих зв'язків, щоб розвивати та оцифровувати свій бізнес, продавати свою продукцію та отримувати інформацію про новини та події у своїх галузях.

Яка б не була архітектура корпоративного середовища, питання щодо забезпечення кібербезпеки залишаються. Тож надалі розглянемо які загрози можуть бути в таких системах організацій.

1.2. Аналіз загроз від шкідливих програм в корпоративному середовищі організацій.

Зловмисне програмне забезпечення (шкідливі програми) – це термін, який використовується для опису шкідливих програм і коду, які можуть завдати шкоди та порушити нормальне використання пристроїв. Зловмисне програмне забезпечення може надавати несанкціонований доступ, використовувати системні ресурси, викрадати паролі, блокувати ваш комп'ютер і вимагати викуп тощо.

Кіберзлочинці, які поширюють зловмисне програмне забезпечення, часто керуються грошима та використовують заражені комп'ютери для здійснення атак, отримання банківських облікових даних, збору інформації, яку можна продати, продажу доступу до комп'ютерних ресурсів або вимагання від жертви грошей [3].

Існує багато типів зловмисного програмного забезпечення, зокрема:

- майнери;
- експлойти та набори експлойтів;
- зловмисне програмне забезпечення для макросів;
- фішинг;
- програми-вимагачі;
- руткіти;
- атаки на ланцюги поставок;
- шахрайство служби технічної підтримки;
- трояни;
- небажане програмне забезпечення;
- черви.

Віруси

Вірус зазвичай надходить у вигляді вкладення в електронному листі, що містить вірусне навантаження або частину шкідливого програмного забезпечення, яке виконує зловмисну дію. Як тільки жертва відкриває файл, пристрій заражається.

Програми-вимагачі

Одним із найприбутковіших і, отже, одним із найпопулярніших видів шкідливих програм серед кіберзлочинців є програми-вимагачі. Це зловмисне програмне забезпечення встановлюється на комп’ютер жертви, шифрує їхні файли, а потім повертається та вимагає викуп (зазвичай у біткойнах) за повернення цих даних користувачеві.

Відлякувальні програми

Кіберзлочинці лякають нас, змушуючи думати, що наші комп’ютери чи смартфони заражені, щоб переконати жертв придбати підроблену програму. У типовому шахрайському програмному забезпеченні під час перегляду веб-сторінок ви можете побачити тривожне повідомлення «Увага: ваш комп’ютер заражено!» або «У

вас вірус!» Кіберзлочинці використовують ці програми та неетичну рекламну практику, щоб залякати користувачів і змусити їх придбати шахрайські програми.

Черви

Черв'яки мають здатність копіювати себе з машини на машину, як правило, використовуючи певну слабкість безпеки програмного забезпечення чи операційної системи, і не вимагають взаємодії користувача для функціонування.

Шпигунське програмне забезпечення

Шпигунське програмне забезпечення – це програма, встановлена на вашому комп’ютері, зазвичай без вашого явного відома, яка збирає та передає користувачеві особисту інформацію чи звички та деталі перегляду Інтернету. Шпигунське програмне забезпечення дозволяє користувачам контролювати всі форми зв’язку на цільовому пристрої. Шпигунське програмне забезпечення часто використовується правоохоронними органами, урядовими установами та організаціями з інформаційної безпеки для тестування та моніторингу комунікацій у конфіденційному середовищі або під час розслідування. Але шпигунське програмне забезпечення також доступне для споживачів, дозволяючи покупцям стежити за своєю дружиною, дітьми та співробітниками.

Трояни

Трояни маскуються під нешкідливі програми, обманом змушуючи користувачів завантажувати та використовувати їх. Після того, як вони запущені, вони можуть викрасти особисті дані, вивести з ладу пристрій, стежити за діяльністю або навіть здійснити атаку.

Рекламне ПЗ

Рекламні програми надсилають небажану рекламу користувачам і зазвичай відображають миготливі рекламні повідомлення або спливаючі вікна, коли ви виконуєте певну дію. Програми з рекламним програмним забезпеченням часто встановлюються в обмін на іншу послугу, наприклад, право використовувати програму без плати за неї.

Безфайлове шкідливе програмне забезпечення

Безфайлове зловмисне програмне забезпечення – це тип шкідливого програмного забезпечення, яке використовує законні програми для зараження комп'ютера. Безфайлові атаки на реєстр зловмисних програм не залишають жодних файлів зловмисного програмного забезпечення для сканування та виявлення зловмисних процесів. Він не покладається на файли та не залишає слідів, тому його складно виявити та видалити.

В IT шкідливе програмне забезпечення або зловмисне програмне забезпечення (складне слово, що складається зі шкідливих і програмних засобів) стосується всіх типів програм, призначених для виконання шкідливих або небажаних дій у системі. До них відносяться комп'ютерні віруси, хробаки, трояни, програми-вимагачі, шпигунські програми та багато інших цифрових шкідників. Як правило, кіберзлочинці використовують ці шкідливі інструменти, щоб отримати доступ до конфіденційних даних, вимагати викуп або просто завдати якомога більшої шкоди ураженій системі. Зараз зловмисне програмне забезпечення здебільшого поширюється через Інтернет. Зловмисники використовують спам із зараженими вкладеними файлами або маніпульовані веб-сайти для розповсюдження шкідливого програмного забезпечення [3].

Зловмисне програмне забезпечення впливає як на приватних, так і на професійних користувачів у всіх галузях і розмірах компаній – часом хакери досягають більшого чи меншого успіху, залежно від цифрової компетенції постраждалих осіб. Ті, хто постійно оновлюють свої системи та завжди критично перевіряють вміст мережі та електронні листи, мають набагато менше страху, ніж користувачі, які мимоволі переглядають Інтернет за допомогою застарілих операційних систем і браузерів. Тим не менш, зараження шкідливим програмним забезпеченням ніколи не можна повністю виключити; однак різноманітні передові методи допомагають мінімізувати площу атаки для зловмисного програмного забезпечення.

Зловмисне програмне забезпечення не робить різниці між галузями та компаніями. У великих кампаніях кіберзлочинці використовують підхід розкидання, щоб рівномірно розподілити зловмисне програмне забезпечення між комп'ютерами невеликих стартапів, малих і середніх підприємств і великих корпорацій у кожній галузі. Державні установи та інші організації також не застраховані від шкідливих програм.

Однак набагато небезпечнішими, ніж широкомасштабні хвилі атак, є цілеспрямовані атаки, спрямовані на конкретну компанію чи одну ціль. У таких сценаріях зловмисники вкладають багато зусиль у підготовку та виконання атак. Наприклад, цільове середовище детально аналізується, щоб виявити слабкі місця в мережах і системах. За цим аналізом слідує фактична атака, яка зазвичай передбачає поєднання соціальної інженерії, фішингу та зловмисного програмного забезпечення. Такі професійні атаки використовуються для проникнення в системи та мережі, що містять дуже чутливі та, отже, надзвичайно цінні дані.

Розглянемо статистику та факти щодо шкідливих програм за 2023 рік.

Зловмисне програмне забезпечення все ще є серйозною проблемою в усьому світі, але природа шкідливого програмного забезпечення змінюється. Ось деякі з найважливіших уявлень про розвиток зловмисного програмного забезпечення у 2022 році.

Зловмисне програмне забезпечення» описує будь-яку шкідливу програму, створену для спустошення комп'ютерної системи. Завдяки постійній взаємодії між професіоналами безпеки та кіберзлочинцями, це також екосистема, що постійно розвивається. Зміни в середовищі зловмисного програмного забезпечення змінюються щороку, хоча довгострокові тенденції можна визначити в річних звітах даних.

Незважаючи на численні заходи боротьби зі зловмисним програмним забезпеченням, кіберзлочинці та хакери не здаються швидко, особливо до тих пір, поки на зловмисному програмному забезпеченні можна заробити гроші. Деякі традиційно популярні форми зловмисного програмного забезпечення, схоже,

втрачають свою популярність у 2022 році, оскільки кіберзлочинці змінюють тактику атаки на нові або недостатньо використовувані вразливості.

Наразі ознаки вказують на те, що хакери зміщують свою увагу на дискретне зараження через Інтернет речей та електронну пошту. Постійно зосереджується увага на корпоративних компаніях і урядах порівняно з пересічними користувачами Інтернету, особливо коли йдеться про зараження програмами-вимагачами.

Ось короткий виклад найцікавішої статистики зловмисного програмного забезпечення:

1. Співробітники з інфікованими машинами поширюють віруси ширше

У 2020 році 61 відсоток організацій стикалися зі зловмисним програмним забезпеченням, яке поширювалося від одного співробітника до іншого. У 2021 році це число зросло до 74 відсотків, а в 2022 році досягло 75 відсотків — це найвищий рівень зараження з початку дослідження SOES у 2016 році.

Збільшення поширення шкідливого програмного забезпечення між працівниками може бути однією з багатьох причин; наприклад, фішингові атаки стають все більш витонченими, а в той же час співробітники можуть зіткнутися з більшою кількістю відволікань під час роботи вдома.

2. Атаки програм-вимагачів часто призводять до зриву бізнесу

У своєму звіті про стан безпеки електронної пошти за 2020 рік Mimecast виявив, що 51% організацій зазнали атаки програм-вимагачів, яка призвела до принаймні часткового порушення бізнес-операцій. У 2021 році цей показник зріс до 61% організацій .

У своєму останньому звіті Mimecast змінив формулювання, тому ми не можемо безпосередньо порівняти результати цього року. Тим не менш, у 2022 році 35 відсотків респондентів звинувачували в кібератаках низький рівень кіберстійкості.

3. Організації в США є одними з найбільш підготовлених до кібератак

Організації в усьому світі повідомляють про атаки програм-вимагачів, які впливають на бізнес, але, здається, компанії в США все більше готові: 47 відсотків

мають стратегії кібер-стійкості. Однак у таких місцях, як Нідерланди, лише 21 відсоток компаній мають план боротьби з будь-якими кібератаками, з якими вони можуть зіткнутися.

4. Майже 70% організацій можуть мати нестачу команд з кібербезпеки

У своєму звіті про стан кібербезпеки за 2022 рік ISACA виявила, що 69 відсотків фахівців з кібербезпеки вважають, що команда з кібербезпеки їхніх організацій неукомплектована, порівняно з 61 відсотком минулого року. Нестача персоналу в організаціях, зокрема в підприємствах і уряді, може створити навантаження на наявний персонал і призвести до підвищеного ризику загроз зловмисного програмного забезпечення.

Майже половина (47 відсотків) повідомили, що їхні організації мають «дещо» нестачу персоналу, тоді як 15 відсотків повідомили, що вони «значно» нестачу персоналу. Ще 34 відсотки повідомили, що в їхній організації «відповідно» укомплектовано персонал, тоді як лише три відсотки повідомили про «дещо» або «значно» надлишок персоналу.

Попит на працівників також зростає з року в рік. Вакансії в індустрії кібербезпеки продовжують залишатися незаповненими, оскільки попит випереджає зростання кількості працівників із необхідними навичками, починаючи від керівників вищих навчальних закладів і закінчуючи технічними спеціалістами та співробітниками.

Рис.1.6. Статистики настачі кадрів з кібербезпеки

5. Тенденції шкідливого програмного забезпечення швидко змінюються

Звіт SecureList IT Threat Evolution за другий квартал 2022 року показує, як продовжує розвиватися зловмисне програмне забезпечення за наймом. У ньому підкреслюється, що організовані групи все частіше розробляють кросплатформне шкідливе програмне забезпечення, щоб скомпрометувати якомога більше систем у цільовій мережі.

У цьому звіті також висвітлюються вразливості в інструментах ведення журналів Windows, які нещодавно відродилися (найвідоміший у скандалі з Log4J, коли організації намагалися виправити величезну кількість різних програм).

6. Фішингові сайти зараз є неймовірно популярним методом атаки

Фішингові сайти зазвичай створені так, щоб виглядати як офіційні версії інших веб-сайтів. PayPal — це сайт, який часто імітують , наприклад, оскільки отримання доступу до облікових даних користувачів PayPal може бути дуже прибутковим для хакерів. Банківські та соціальні мережі також є досить поширеними цілями.

Докладніше: 70+ поширених онлайн-шахрайств, якими користуються кіберзлочинці.

7. Google продовжує придушувати потенційно шкідливі сайти

Відповідно до Звіту Google про прозорість , 3,849 мільйона попереджень браузера було показано користувачам, які намагалися отримати доступ до сайтів, які безпечний перегляд визнав небезпечними. станом на 7 серпня 2022 р. Крім того, 1,6 мільйона користувачів побачили попередження в результатах пошуку про те, що сайт , який вони збираються відвідати, може бути шкідливим.

Якщо ми дослідимо загальні дані, то побачимо, що за останнє десятиліття кількість попереджень різко зменшилася. Це навряд чи тому, що існує менше небезпечних сайтів; скоріше, Google став краще їх ідентифікувати та видаляти з результатів, що призвело до меншої кількості попереджень.

8. Кількість атак шкідливих програм знову зростає

У 2020 році кількість нових атак зловмисного програмного забезпечення зменшилася вперше з 2015 року. Однак, згідно зі звітом SonicWall про кіберзагрози за 2022 рік , це було лише тимчасовим падінням: зараз кількість атак зловмисного програмного забезпечення становить 10,4 мільйона на рік, приблизно на тому місці, де вони були раніше. у 2018 році.

Статистика зловмисного програмного забезпечення та факти

«Зловмисне програмне забезпечення» описує будь-яку шкідливу програму, створену для спустошення комп’ютерної системи. Завдяки постійній взаємодії між професіоналами безпеки та кіберзлочинцями, це також екосистема, що постійно розвивається. Зміни в середовищі зловмисного програмного забезпечення змінюються щороку, хоча довгострокові тенденції можна визначити в річних звітах даних.

Незважаючи на численні заходи боротьби зі зловмисним програмним забезпеченням, кіберзлочинці та хакери не здаються швидко, особливо до тих пір, поки на зловмисному програмному забезпеченні можна заробити гроші. Деякі традиційно популярні форми зловмисного програмного забезпечення, схоже, втрачають свою популярність у 2022 році, оскільки кіберзлочинці змінюють тактику атаки на нові або недостатньо використовувані вразливості.

9. З року в рік кількість нових варіантів шкідливого програмного забезпечення зменшується.

SonicWall повідомила про 5,4 мільярда атак зловмисного програмного забезпечення у 2021 році, що звучить погано, але насправді є невеликим зменшенням порівняно з попереднім роком. Ми ще не маємо повних даних за 2022 рік, але за перші шість місяців було зафіксовано 2,75 мільярда атак, і якщо ці цифри збережуться, ми отримаємо приблизно таку ж річну кількість атак.

10. Алгоритми генерації домену все ще перешкоджають зусиллям із захисту від шкідливих програм

Алгоритми генерації домену, або DGA, дозволяють архітекторам зловмисного програмного забезпечення автоматично генерувати велику кількість доменних імен, які потім служать точками зустрічі для контролю та збору даних про активні зараження шкідливим програмним забезпеченням. DGA ускладнюють розслідування та аналіз, що, у свою чергу, ускладнює закриття ботнетів.

Понад 40 сімейств шкідливих програм використовують DGA, у тому числі добре відомі шкідливі програми, зокрема CCleaner, Emotet і Mirai. У 2019 році SonicWall виявив понад 172 мільйони випадково згенерованих доменів.

11. Атаки шкідливих програм на нестандартні порти впали на 10 відсотків

У звіті SonicWall за 2022 рік виявлено, що атаки на десятки тисяч доступних нестандартних портів зменшилися до дев’яти відсотків у 2021 році. Це значне падіння порівняно з минулим роком і фактично найнижчий рівень захворюваності з 2019 року. Переважна більшість атак все ще (і швидше за все залишиться) проблема стандартних портів, таких як HTTP (порт 80).

12. Програми-вимагачі та зловмисне програмне забезпечення Інтернету речей поширені як ніколи

Звіт SonicWall за півріччя 2022 року показує, що кількість програм-вимагачів фактично зменшилася з року в рік, у середньому близько 40 мільйонів атак на місяць (зниження з 50,5 мільйонів у першому півріччі 2021 року).

Однак важливо розуміти, що ці цифри вже значно вищі, ніж у попередні роки, головним чином через вибух програм-вимагачів, який стався під час пандемії COVID-19.

13. У першому півріччі 2022 року було виявлено понад 270 000 нових варіантів шкідливого ПЗ

Лише за першу половину 2022 року SonicWall виявив 270 228 «ніколи раніше не бачених» варіантів шкідливого програмного забезпечення. Це на 45 відсотків більше, ніж за той же період минулого року, і в середньому становить понад 1500 абсолютно нових варіантів щодня. Тільки в березні було виявлено майже 60 тисяч нових варіантів, що є новим рекордом.

14. Cerber є найпопулярнішою сигнатурою програм-вимагачів першого півріччя 2022 року

У першій половині 2022 року Cerber повернув собі корону найпоширенішого програмного забезпечення-вимагача. Раніше Ryuk посунув його на друге місце, але тепер ситуація знову змінилася: Cerber присутній у 43 мільйонах заражень. SamSam, який раніше був ще одним головним претендентом, був виведений із трійки лідерів GandCrab, хоча група, що стоїть за цим, офіційно закрила магазин у 2019 році.

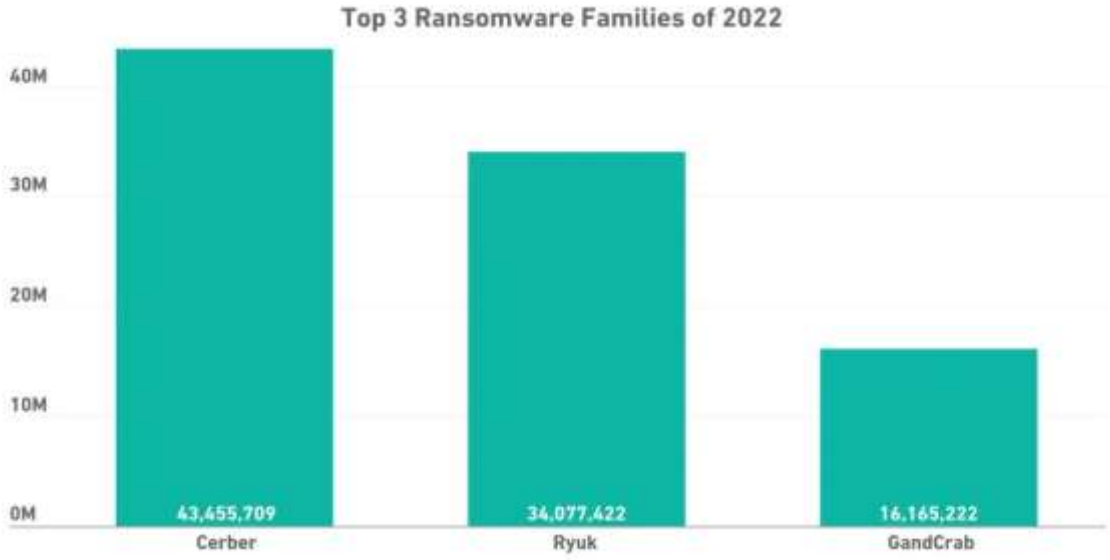


Рис.1.7. Атаки програм-вимагачів

SonicWall найкращі сімейства програм-вимагачів 2022

15. 60% усіх атак зловмисного програмного забезпечення було надіслано з використанням зашифрованого трафіку.

Зловмисники люблять надсилати атаки зловмисного програмного забезпечення через зашифрований трафік SSL/TLS. Зашифровані канали ускладнюють виявлення та попередження, що призводить до вищих показників успішності пакетів зловмисного програмного забезпечення. Проте WatchGuard повідомив, що в першому кварталі 2022 року 60,1 відсотка всіх виявлених зловмисних програм були атаками такого характеру, порівняно з 91 відсотком у другому кварталі 2021 року.

16. Підприємства є основною мішенню для програм-вимагачів

Coveware зазначив, що професійні послуги були найпоширенішими цілями програм-вимагачів у другому кварталі 2022 року, на них припадало 21,9 відсотка всіх атак (порівняно з 20,2 відсотка в попередньому кварталі).

Далі йдуть організації державного сектору (14,4 відсотка), медичні організації — 10 відсотків, а послуги програмного забезпечення — 9,4 відсотка. Фінансові установи були значно менш популярні в цьому кварталі, впавши з 8,9 відсотка до 6,4 відсотка всього за три місяці.

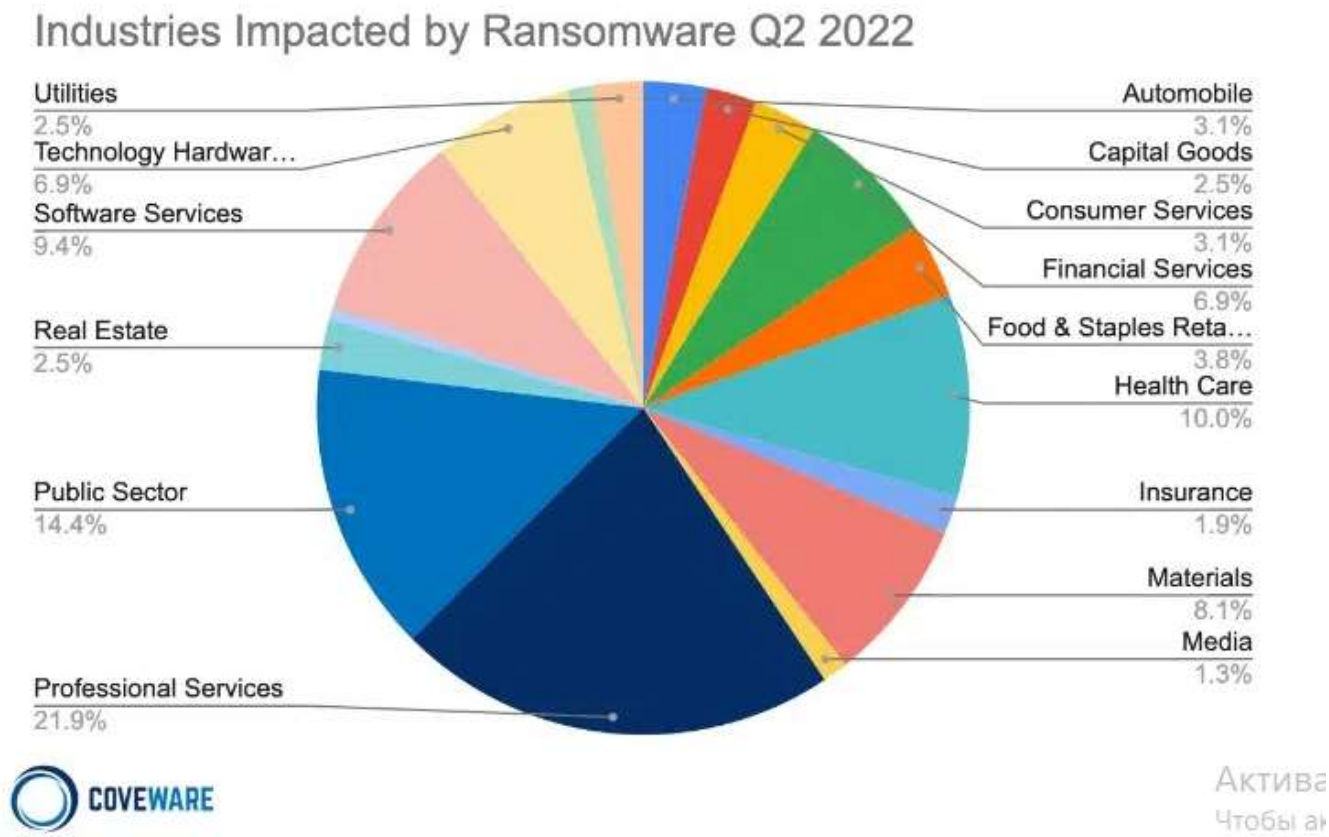


Рис.1.8. Жертви програм-вимагачів Q2 2022

Прогнози зловмисного програмного забезпечення на 2023 рік.

Виходячи з цього, можемо очікувати, що побачимо кілька ключових висновків до кінця року:

Сайти, заражені зловмисним програмним забезпеченням, ймовірно, продовжуватимуть втрачати популярність і зменшуватимуться обсяги.

Кіберзлочинці продовжуватимуть націлюватися на великі підприємства за допомогою шкідливого програмного забезпечення в надії отримати велику одноразову виплату.

Вимагана сума платежу за програми-вимагачі продовжуватиме збільшуватися.

Загроза шифрування для пристроїв IoT зростатиме, не в малу частину завдяки зростанню кількості незахищених пристроїв IoT, які споживачі купують у дедалі більшій кількості.

Також увагу необхідно зосередити на впроваджені рішень, щодо захисту корпоративного середовища від шкідливих програм.

1.3. Аналіз рішень для вибору рішень захисту від шкідливих програм

Проведемо аналіз рішень захисту від шкідливих програм від провідних компаній.

Першою проаналізуємо ESET Endpoint Security. Дане рішення використовує багаторівневий підхід з багатьма технологіями для збалансованого поєднання високої продуктивності, точності виявлення та уникнення помилкових спрацювань. Зміцнює безпеку компанії за допомогою технологій [5]:

– захист від програм-вимагачів;
– блокування цілеспрямованих атак;
– запобігання втратам даних;
– запобігання атакам без використання файлів;
– виявлення складних загроз;
– захист мобільних пристроїв та управління ними.

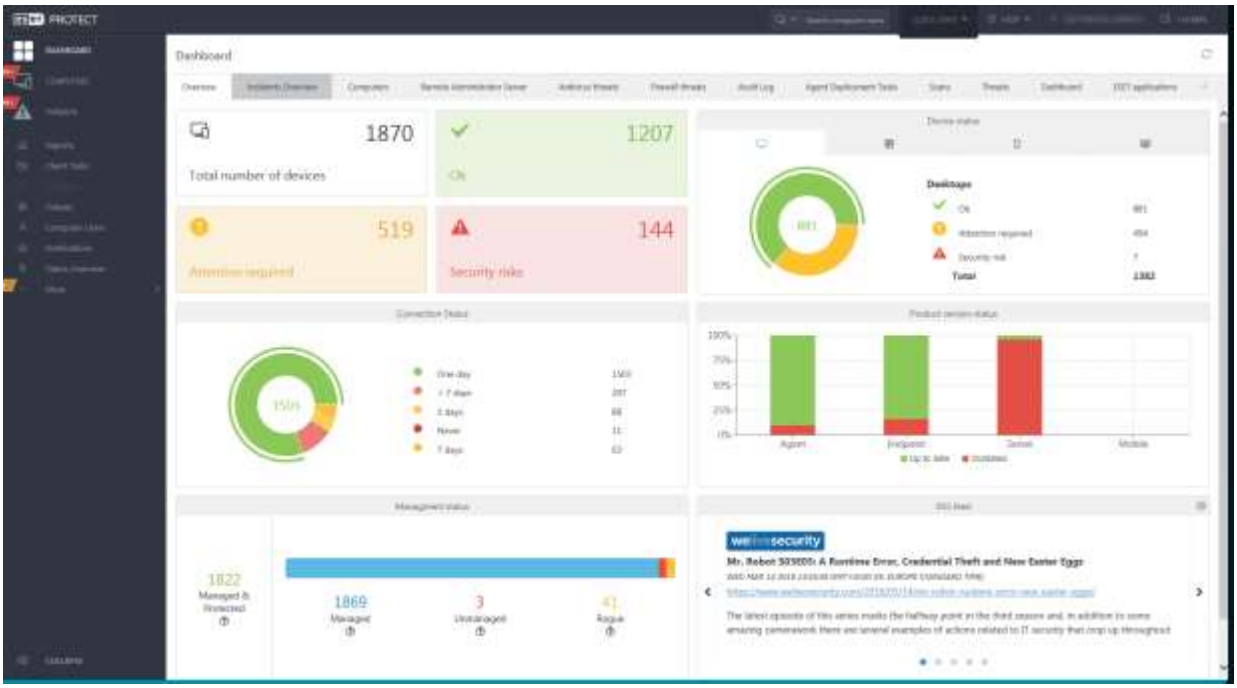


Рис. 1.9. Хмарна консоль ESET PROTECT [6]

Основні переваги ESET Endpoint Security включають:

- управління з єдиної консолі

Усіма продуктами ESET для захисту робочих станцій, у тому числі мобільних пристроїв, можна управляти з єдиної локальної або хмарної консолі ESET PROTECT [5].

- захист від програм-вимагачів

Надає додатковий рівень захисту користувачів від програм-вимагачів. Технологія контролює та оцінює всі виконані програми на основі їхньої поведінки та репутації, а також завдяки технології Intel® для виявлення загроз забезпечує покращене виявлення програм-вимагачів [6].

- запобігання атакам без використання файлів

Для захисту від атак без використання файлів рішення ESET для захисту робочих станцій виявляють додатки, які можуть несанкціоновано використовуватись зловмисниками. [6].

- блокування цілеспрямованих атак

Рішення ESET використовують інформацію про глобальне поширення загроз для визначення пріоритетів та ефективного блокування нових загроз, попереджаючи їх подальше розповсюдження у світі [6].

- захист веб-браузера

Цей спеціальний рівень захисту зосереджується на захисті браузера, який є основним інструментом для доступу до важливих даних усередині периметра Інтранет-мережі та у хмарі [6]/

- захист від атак методом підбору паролів

Виявляє та блокує автоматизовані атаки, які використовують методи підбору пароля для отримання доступу до вашої мережі [6].

Друге рішення, яке проаналізуємо – це Avira Prime [7]. Дане рішення забезпечує максимальну безпеку для малого та середнього бізнесу, забезпечуючи повний захист

кінцевих точок. Конфіденційність захищена, коли користувачі в мережі, а їх пристрої мають оптимізовану швидкість і продуктивність.

Рішення постачається з Avira Protection Cloud, гібридом таких технологій, як штучний інтелект, механізми багаторазового сканування, аналіз поведінки та ройовий інтелект. Поєднуючи всі ці функції, Avira забезпечує найкращий захист від численних загроз, таких як фішингові атаки, програми-вимагачі та шкідливі програми [7].

Програмне забезпечення безпеки — це міжплатформне рішення, яке може вирішити велику кількість проблеми з конфіденційністю до 25 ваших пристроїв, включаючи Windows, Mac, веб-браузери, Android та iOS.

Має більше функцій і переваг.

Розумне сканування

Дозволяє просканувати всю систему на наявність зловмисного програмного забезпечення, слабких паролів, невиправленого або застарілого програмного забезпечення та мережевих вразливостей одним клацанням миші.

Антивірусний захист

Рішення виявляє та захищає всі і кінцеві точки від зловмисного програмного забезпечення та онлайн-загроз у режимі реального часу.

Безлімітний VPN

Інструмент захищає ваші бізнес-дані та забезпечує безпеку в Інтернеті за допомогою необмеженого VPN, а також забезпечує розширені налаштування конфіденційності для захисту конфіденційних бізнес-даних.

Очищувач ПК

Avira може оптимізувати ваш цифровий досвід, очищаючи непотрібні файли, що зменшує пам’ять. Це може пришвидшити час завантаження, зменшити затримку та підвищити загальну продуктивність.

Керування паролями

Дозволяє створювати надбезпечні паролі та керувати ними для всіх облікових записів вашого бізнесу в Інтернеті.

Проаналізуємо ще одну тезнологіюAcronis Cyber Protect.

Acronis Cyber Protect використовує на основі штучного інтелекту статичні, поведінкові евристичні антивірусні технології, технології захисту від зловмисного програмного забезпечення та програм-вимагачів для захисту ваших даних у режимі реального часу [7].

Завдяки Acronis Cyber Protect є можливість отримами безперервний моніторинг і сповіщення в режимі реального часу про зловмисне програмне забезпечення, уразливості, стихійні лиха та сповіщення про потенційні глобальні загрози будь-якого роду, які можуть поставити під загрозу безпеку даних, щоб ви могли вжити заходів [7].

Крім того, завдяки рішенню є можливість сканувати свої пристрої на наявність вразливостей за допомогою функції оцінки вразливостей Acronis, щоб гарантувати, що всі програми та операційні системи оновлені та не можуть бути використані хакерами.

Іншою корисною функцією є запобігання експлойтам, яке допомагає зупинити та запобігти атакам за допомогою таких інструментів, як захист від ескалації привілеїв, захист пам’яті, захист від впровадження коду та захист від зворотного програмування.

Більше функцій і переваг

Резервне копіювання файлів і образів дисків

Рішення автоматично створює резервні копії окремих даних або захищає всю вашу організацію, створюючи резервну копію всієї системи як одного файлу. Це дозволяє легко відновити всю інформацію на новому апаратному забезпеченні у разі збою даних.

Постійний захист даних

Агент Acronis складає список критичних програм, які користувачі зазвичай часто використовують, і постійно створює резервні копії кожної зміни, внесеної в перелічені програми, незалежно від того, де користувач зберіг файл, гарантуючи, що

користувачі не втратять незавершену роботу. Якщо систему потрібно повторно створити, ви можете відновити дані з резервної копії та застосувати останні зміни, гарантуючи, що дані не буде втрачено.

Моніторинг здоров'я диска

Інструмент може попередити вас про проблему з диском ще до того, як вона виникне, оскільки використовує різні параметри операційної системи, такі як звіти про сповіщення та машинне навчання, щоб постійно відстежувати стан вашого диска. Це дає змогу вжити необхідних заходів безпеки для захисту ваших даних, що допоможе уникнути випадкової втрати даних, а також збільшити час безвідмовної роботи.

Сканування резервних копій на захист від шкідливих програм

Він має вбудований сканер зловмисного програмного забезпечення, який запобігає відновленню інфікованих файлів шляхом сканування резервних копій повного диска в централізованому місці, гарантуючи, що ви відновите лише чисту резервну копію без шкідливих програм.

Збір судово-медичних даних

Також є вбудований режим Forensic Mode для збору цифрових доказів, таких як дампи пам'яті та інформація про процес, із резервних копій на рівні диска. Збір цифрових доказів допоможе спростити майбутній аналіз.

Дистанційно стирає дані з пристроїв

Ще одна функція — вона дозволяє дистанційно стирати зламані або відсутні пристрої Windows. Це означає, що ви можете успішно запобігти видаленню даних зловмисниками або доступу кіберзлочинців через втрачені чи викрадені пристрої.

В результаті аналізу, для подальшого дослідження методів та засобів захисту від шкідливих програм обираємо Acronis Cyber Protect.

2 МЕТОДИ ТА ЗАСОБИ ЩОДО ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ КОРПОРАТИВНЕ СЕРЕДОВИЩЕ НА БАЗІ ACRONIS

2.1 Призначення та функції рішення Acronis Cyber Protect

Acronis Cyber Protect — комплексне рішення щодо кіберзахисту, в якому поєднано функції захисту даних та кібербезпеки. Воно забезпечує інноваційну комбінацію наступних можливостей:

Проактивний захист: оцінка вразливостей та управління виправленнями; прогнозний аналіз стану жорсткого диска з урахуванням технологій машинного навчання; видалення шкідливих програм із резервних копій; недопущення інфікувань, що повторюються.

Активний захист: безперервний захист даних (CDP), захист від програм-вимагачів та шкідливих програм; самозахист.

Захист у відповідь : резервне копіювання та відновлення повного образу/рівні файлів; миттєве відновлення віртуальних машин; створення резервних копій для судових експертиз.

Identify	Protect	Detect	Respond	Recover
Autodiscovery of new devices	Remote agent installation	Protection against malware and exploits	Patch management integrated with backup	Backup and disaster recovery
Vulnerability assessment	Backup and disaster recovery	Disk health forecast	Malware quarantine	Forensic information in backups
Data protection map	Unified management of protection plans	Dashboards and reports	Rescue with bootable media	Remote desktop

Function areas are grouped according to the NIST Cybersecurity Framework

Рис.2.1. Функції Acronis Cyber Protect відповідно NIST

Основні функції Acronis Cyber Protect включають:

Резервне копіювання та відновлення. Резервне копіювання та відновлення фізичних машин, віртуальних машин та додатків.

Аварійне відновлення. Захищає локальне середовище при виникненні аварійних ситуацій шляхом запуску точних копій машин у хмарі та перемикання робочого навантаження на сервери хмар.

Захист від шкідливих програм та веб-захист. Захищає машини від усіх нових загроз з боку шкідливих програм, запобігє завантаженню шкідливих файлів і блокє доступ до підозрілих веб-ресурсів.

Автоматичне виявлення машин. Автоматична реєстрація великої кількості машин та встановлення агента захисту та додаткових компонентів.

Оцінка вразливостей. Сканує операційні системи та програми на наявність уразливостей.

Управління виправленнями. Підтверджує виправлення автоматично або вручну, планує установки виправлень або запускає їх на вимогу, задає гнучкі параметри перезапуску та вікна обслуговування, використовує поетапне розгортання.

Моніторинг працездатності диска. Відстеження стану жорстких дисків та недопущення їхнього несподіваного виходу з ладу.

Віддалене управління та підтримка. Підключається до машин та керує ними віддалено.

Acronis Cyber Protect підтримує інноваційні сценарії захисту даних, які включають в себе:

Безперервний захист даних (CDP). Виключає навіть мізерну втрату даних у основних додатках.

Надійна установка виправлень. Автоматично створює резервні копії машин перед встановленням на них будь-яких виправлень, щоб мати можливість виконати відкат негайно (за потреби).

Найкращий захист з використанням меншої кількості ресурсів. Розвантажує систему та забезпечує більш розширене сканування та оцінку вразливостей у центральному сховищі даних, включаючи хмару.

Резервні копії для судових експертиз. Увімкніть до складу резервних копій електронні докази, які дозволять спростити та прискорити розслідування.

Карта захисту даних. Відстежує статус захисту файлів завдяки класифікації, звітності та аналітиці неструктурованих даних.

Безпечне відновлення. Інтегрує оновлення для захисту від шкідливих програм та виправлення у процес відновлення.

Інтелектуальний план захисту. Автоматичное налаштовує виправлення, сканування та резервного копіювання на основі оповіщень із Cyber Protection Operations Center.

Глобальні та локальні білі списки Створює білі списки на основі резервних копій, щоб покращити евристику та уникнути помилкових виявлень.

Acronis Cyber Protect доступний у кількох версіях, щоб точніше задовольняти потреби різних груп клієнтів:

• Acronis Cyber Protect Essentials – забезпечує необхідний кіберзахист за доступною ціною, щоб малий і середній бізнес з меншими бюджетами на кібербезпеку міг захистити свої дані. Включає базові можливості резервного копіювання на рівні файлів і основні функції кіберзахисту, такі як захист від вірусів і шкідливих програм, оцінка вразливостей, керування виправленнями та фільтрація URL-адрес.

• Acronis Cyber Protect Standard – призначений для малих і середніх підприємств, яким потрібні стандартні функції резервного копіювання та багаторівневий кіберзахист від будь-яких загроз. Включає комплексний захист даних плюс додаткові можливості кібербезпеки, такі як карти захисту даних, фільтрація URL-адрес і категоризація, постійний захист даних і працездатність жорсткого диска.

• Acronis Cyber Protect Advanced – розроблений для підприємств, які використовують більші та складніші середовища. Включає розширені можливості

резервного копіювання та кібербезпеки, такі як підтримка додаткових робочих навантажень, спільні плани захисту, нотаріальне засвідчення резервних копій, безпечне відновлення резервних копій, сканування резервних копій на наявність зловмисного програмного забезпечення, конфігурація інформаційної панелі та оцінка стану безпеки.

• Acronis Cyber Protect — Backup Advanced — розроблений для підприємств, які використовують великі середовища з більшою кількістю користувачів і складнішою інфраструктурою. Включає захист даних від програм-вимагачів і криптомайнінгу, а також розширені функції резервного копіювання, такі як: керування групами, спільні плани захисту, обробка даних поза хостом, підтримка стрічки, дедуплікація та настроювані звіти.

2.2. Архітектура та складові модулі Acronis Cyber Protect

Розглянемо архітектуру та основні модулі рішення Acronis Cyber Protect (рис.2.1).

Сервер керування є центральним компонентом Acronis Cyber Protect. Він надає два порти TCP: 7780 і 9877. Порт 9877, захищений TLS, використовується для надання як REST API, так і веб-інтерфейсу користувача. Кінцеві точки REST API автентифікують запити за допомогою токенів JWT, представлених у вигляді окремого заголовка HTTP або закодованих як файл cookie HTTP. Порт 7780 реалізує протокол ZeroMQ з автентифікацією та шифруванням ZMTP CURVE. Порт 7780 використовується агентами та вузлом зберігання для асинхронного обміну повідомленнями керування з сервером керування. Сервер керування також спілкується з хмарними службами для завантаження оновлень через стандартні порти HTTP та HTTPS.

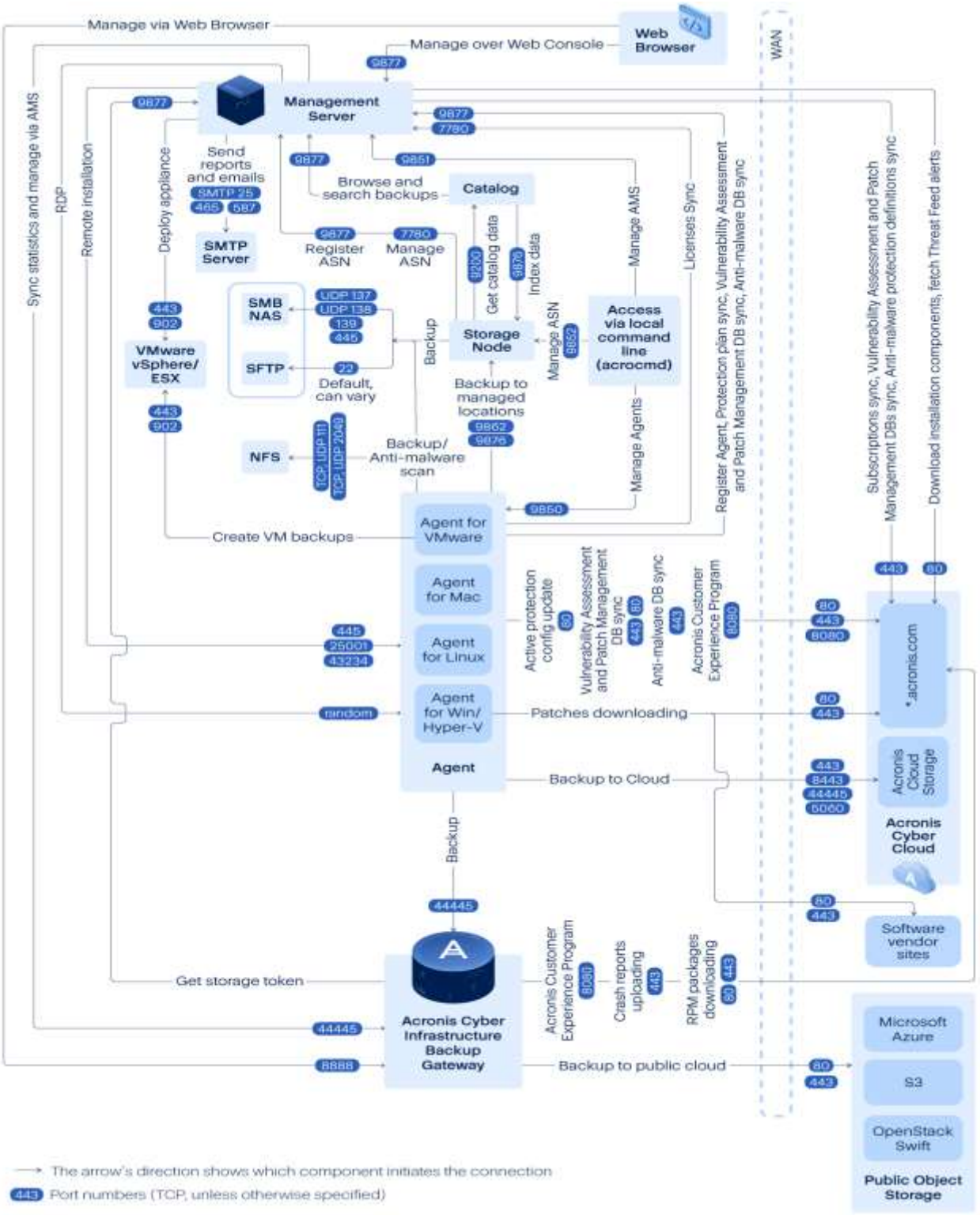


Рис. 2.2. Архітектура та модулі Acronis Cyber Protect

Вузол зберігання — це компонент зберігання Acronis Cyber Protect. Він відкриває порт TCP 9876. Цей порт використовується для надсилання та отримання

резервних даних. Транспорт захищено TLS, а автентифікація здійснюється за допомогою спільного TLS. Протокол на рівні програми є власністю Acronis. Вузол зберігання спілкується з серверними системами зберігання за допомогою відповідних протоколів і механізмів автентифікації.

Каталог є допоміжним компонентом Acronis Cyber Protect. Він індексує дані на вузлі зберігання, отримуючи до них доступ через порт 9876 і відкриваючи індекс у порту 9200.

Шлюз резервного копіювання реалізує наступне покоління власного протоколу доступу до даних Acronis. Той самий компонент використовується в Acronis Cyber Cloud, якщо клієнт погоджується на резервне копіювання в хмарі. Порт TCP 44445, зареєстрований в IANA, використовується шлюзом. Захист даних здійснюється через TLS, а автентифікація здійснюється за допомогою спільного TLS. Резервний шлюз також може використовувати порт 8888 для служби керування на основі HTTPS.

Агент зв'язується з сервером керування, вузлом зберігання та резервним шлюзом через порти, як описано вище. Агент також може спілкуватися з файловими службами на основі стандартів (SMB, NFS), якщо вони використовуються як місце призначення для резервного копіювання. У цьому випадку використовуються стандартні порти та відповідні протоколи автентифікації. Агент для VMware використовує API VMware vSphere через порти, визначені VMware vSphere, коли така функція налаштована.

2.3. Методи виявлення шкідливого програмного забезпечення Acronis Cyber Protect

Шкідливе програмне – це програмне забезпечення, метою якого є проникнення на комп'ютер користувача, створення своїх копій і приховане виконання шкідливих дій.

Види шкідливих програм:

безпечні – виявляються з відео та звуковим ефектам. Вони не змінюють файлову систему, не шкодять файли і не виконують ніяких шпигунських дій;

небезпечні - можуть привести до збоїв у роботі комп'ютерної системи. Це може призвести до зменшення розміру доступної оперативної пам'яті, перезавантажувати комп'ютер тощо;

дуже небезпечні – можуть знищити інформацію з пам'яті та виконувати шпигунські дії тощо.

Антивірус - це комплекс програм, призначений для виявлення і знешкодження вредносносного програмного забезпечення, а також для усунення наслідків дій шкідливого програмного забезпечення на комп'ютері.

До основних функції антивірусного програмного забезпечення, а це стосується і шкідливих програм відноситься:

– Моніторинг файлів.

– Перевірка файлів на зараження з метою, локалізації та подальшого лікування.

– Своєчасне оновлення антивірусних баз даних.

Тож, виходячи з визначення, основними завданнями антивірусу є:

– Перешкоджання проникненню шкідливих програму комп'ютерну систему.

– Виявлення наявності шкідливих програм у комп'ютерній системі.

– Усунення вірусів з комп’ютерної системи без нанесення ушкоджень іншим об’єктам системи.

– Мінімізація збитку від дій вірусів.

– Методи виявлення вірусів.

Методи, застосовувані в антивірусах, можна розбити на дві групи:

– Методиї сигнатурного аналізу

– Методи імовірнісного аналізу

Сигнатурний аналіз – метод виявлення вірусів, що полягає в перевірці наявності у файлах сигнатур вірусів.

Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використається практично у всіх сучасних антивірусах. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі. Антивірусна база – база даних, у якій зберігаються сигнатури вірусів.[7]

Через те, що сигнатурний аналіз припускає перевірку файлів на наявність сигнатур вірусів, антивірусна база має потребу в періодичному відновленні для підтримки актуальності антивірусу. Сам принцип роботи сигнатурного аналізу також визначає границі його функціональності – можливість виявляти лише вже відомі віруси – проти нових вірусів сигнатурний сканер неспроможний.

З іншого боку, наявність сигнатур вірусів припускає можливість лікування інфікованих файлів, виявлених за допомогою сигнатурного аналізу. Однак, лікування припустиме не для всіх вірусів – трояни й більшість хробаків не піддаються лікуванню по своїх конструктивних особливостях, оскільки є цільними модулями, створеними для завдання збитків.

Грамотна реалізація вірусної сигнатури дозволяє виявляти відомі віруси зі стовідсотковою ймовірністю. Метод імовірнісного аналізу у свою чергу підрозділяються на три категорії: евристичний аналіз, поведінковий аналіз, аналіз контрольних сум.

Евристичний аналіз – технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об’єктів.У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонам. Найбільш популярною евристичною технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів й їхніх комбінацій. Це допомагає визначати гібриди й нові версії раніше відомих вірусів без додаткового відновлення антивірусної бази. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не припускає лікування.Дана технологія не здатна на 100% визначити вірус перед нею чи ні, і як будь—який імовірнісний алгоритм грішить помилковими спрацьовуваннями.

Поведінковий аналіз – технологія, у якій рішення про характер об’єкта, що перевіряє, приймається на основі аналізу виконуваних їм операцій.Поведінковий аналіз досить вузько застосуємо на практиці, тому що більшість дій, характерних для вірусів, можуть виконуватися й звичайними додатками. Найбільшу популярність одержали поведінкові аналізатори скріптів і макросів, оскільки відповідні віруси практично завжди виконують ряд однотипних дій. Наприклад, для впровадження в систему, майже кожен макровірус використає той самий алгоритм: у який—небудь стандартний макрос, що запускається автоматично середовищем Microsoft Office при виконанні стандартних команд (наприклад, «Save», «Save As», «Open», і т.д.), записується код, що заражає основний файл шаблонів normal.dot і кожен документ, що відкриває знову. Засоби захисту, що вшивають в BIOS, також можна віднести до поведінкових аналізаторів. При спробі внести зміни в MBR комп’ютера, аналізатор блокує дія й виводить відповідне повідомлення користувачеві. Крім цього поведінкові аналізатори можуть відслідковувати спроби прямого доступу до файлів, внесення змін у завантажувальний запис дискет, форматування жорстких дисків і т.д.

Поведінкові аналізатори не використають для роботи додаткових об’єктів, подібних до вірусних баз й, як наслідок, нездатні розрізняти відомі й невідомі віруси – всі підозрілі програми апріорі вважаються невідомими вірусами. Аналогічно,

особливості роботи засобів, що реалізують технології поведінкового аналізу, не припускають лікування. Як й у попередньому випадку, можливе виділення дій, що однозначно трактуються як неправомірні – форматування жорстких дисків без запиту, видалення всіх даних з логічного диска, зміна завантажувального запису дискети без відповідних повідомлень й ін. Проте, наявність дій неоднозначних – наприклад, макрокоманда створення каталогу на жорсткому диску, змушує також замислюватися про помилкові спрацьовування й, найчастіше, про тонке ручне настроювання поведінкового блокатора.

Аналіз контрольних сум – це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін – одночасність, масовість, ідентичні зміни довжин файлів – можна робити висновок про зараження системи. Аналізатори контрольних сум (також використається назва «ревізори змін») як і поведінкові аналізатори не використають у роботі додаткові об'єкти й видають вердикт про наявність вірусу в системі винятково методом експертної оцінки. Більша популярність аналізу контрольних сум пов'язана зі спогадами про однозадачні операційні системи, коли кількість вірусів бути відносно невеликим, файлів було небагато й мінялися вони рідко. Сьогодні ревізори змін втратили свої позиції й використаються в антивірусах досить рідко. Частіше подібні технології застосовуються в сканерах при доступі – при першій перевірці з файлу знімається контрольна сума й міститься в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, рівняється, і у випадку відсутності змін файл уважається незараженим.

Acronis Cyber Protect використовує аналіз поведінки на основі ШІ для виявлення та запобігання зараженню зловмисним програмним забезпеченням. Ця технологія може ідентифікувати зловмисну поведінку, яку можуть не виявити традиційні антивірусні рішення на основі сигнатур.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ НА БАЗІ ACRONIS

3.1. Функції роботи модуля захисту від шкідливих програм

Модуль «Антивірус та захист від шкідливих програм» дозволяє захистити машини Windows та macOS від усіх нових загроз з боку шкідливих програм. В даному рішенні включено Active Protection, але вона не підтримується на машинах macOS.

Якщо машина вже захищена сторонньою антивірусною програмою станом на час застосування до неї модуля «Антивірус та захист від шкідливих програм», система сформує сповіщення та зупинить захист у реальному часі для запобігання потенційним проблемам із сумісністю та продуктивністю. Щоб забезпечити повнофункціональний захист Acronis Cyber Protect від вірусів та шкідливих програм, необхідно буде відключити або видалити сторонню антивірусну програму (рис.3.1).

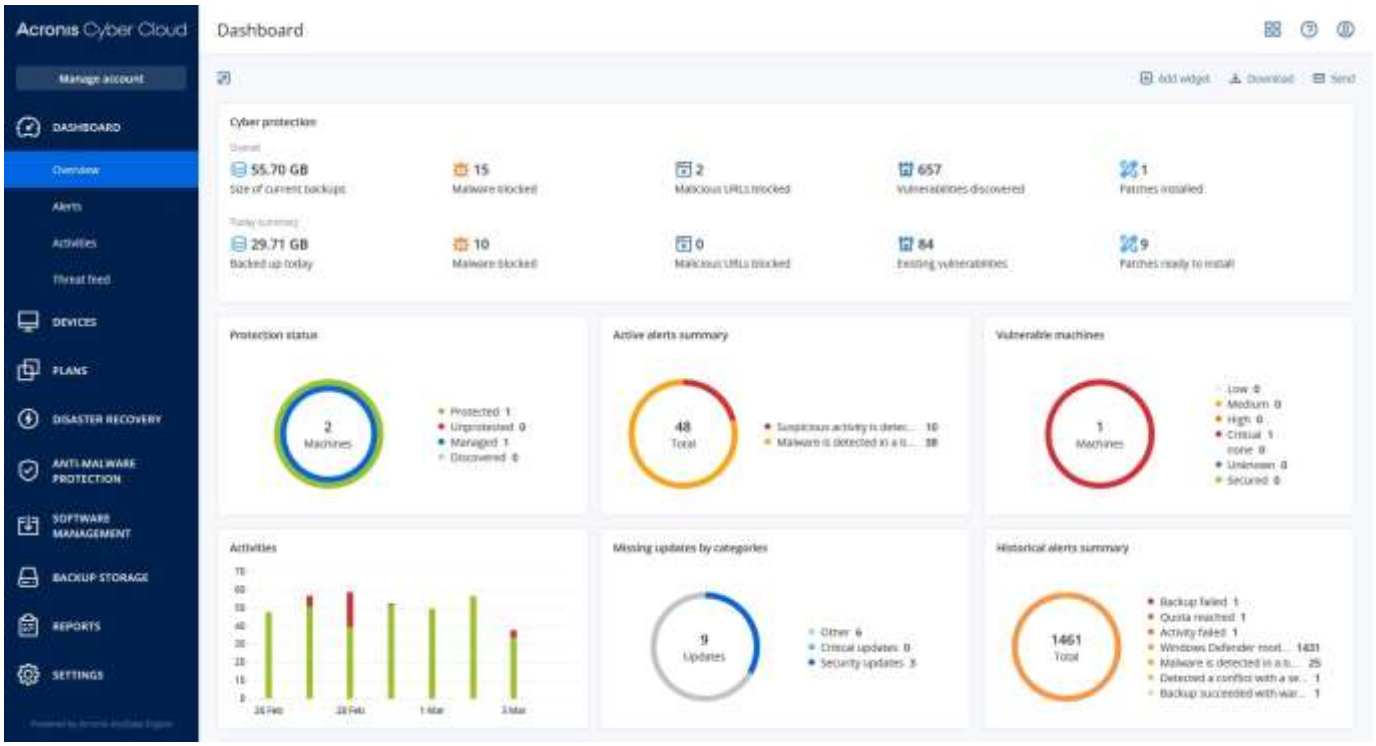


Рис.3.1. Панель рішення Acronis Cyber Protect

Нижче наведемо можливості захисту від шкідливих програм:

Виявлення шкідливих програм у файлах у режимах реального часу та "на вимогу" (для Windows, macOS).

Виявлення шкідливої поведінки у процесах (для Windows).

Блокування доступу до шкідливих URL-адрес (для Windows).

Переміщення небезпечних файлів до карантину.

Додавання довірених корпоративних додатків до білого списку.

Модуль «Антивірус та захист від шкідливих програм» дозволяє виконати сканування двох типів.

Сканування «Захист у реальному часі».

Сканування на шкідливі програми на вимогу.

При скануванні в реальному часі з метою нейтралізації загроз перевіряються всі файли, які запускаються або відкриваються на машині.

Можна вибрати один із наведених нижче видів сканування.

1. Виявлення доступу означає, що у фоновому режимі виконується антишкідлива програма, яка активно і постійно сканує систему на вашій машині на віруси та інші загрози весь час, поки система увімкнена. Шкідливі програми виявляються в обох випадках при виконанні файлу та при виконанні різних операцій із файлом, таких як його відкриття для читання/редагування.

1. Виявлення під час виконання означає, що скануються лише виконувані файли під час їх запуску, щоб перевірити їх у відсутності загроз і щодо безпеки для машини чи даних. Копіювання інфікованого файлу залишиться непоміченим.

Сканування на шкідливі програми на вимогу, це сканування на шкідливі програми виконується відповідно до розкладу або результати сканування на шкідливі програми можна відстежити у віджеті *Панель моніторингу - Огляд -Останні.*

3.2. Рекомендації щодо створення плану захисту Acronis Cyber Protect.

Створення плану захисту

Створення плану захисту дозволяє застосувати до кількох машин під час його створення або пізніше. Коли ви створюєте план, система перевіряє операційну систему та тип пристрою (наприклад, робоча станція, віртуальна машина тощо) і показує лише ті модулі плану, які застосовуються до ваших пристроїв.

План захисту можна створити двома способами:

У розділі «Пристрої» – коли ви вибираєте пристрій або пристрої, які потрібно захистити, а потім створюєте для них план.

У розділі «Плани» – коли ви створюєте план, а потім вибираєте машини, до яких потрібно застосувати.

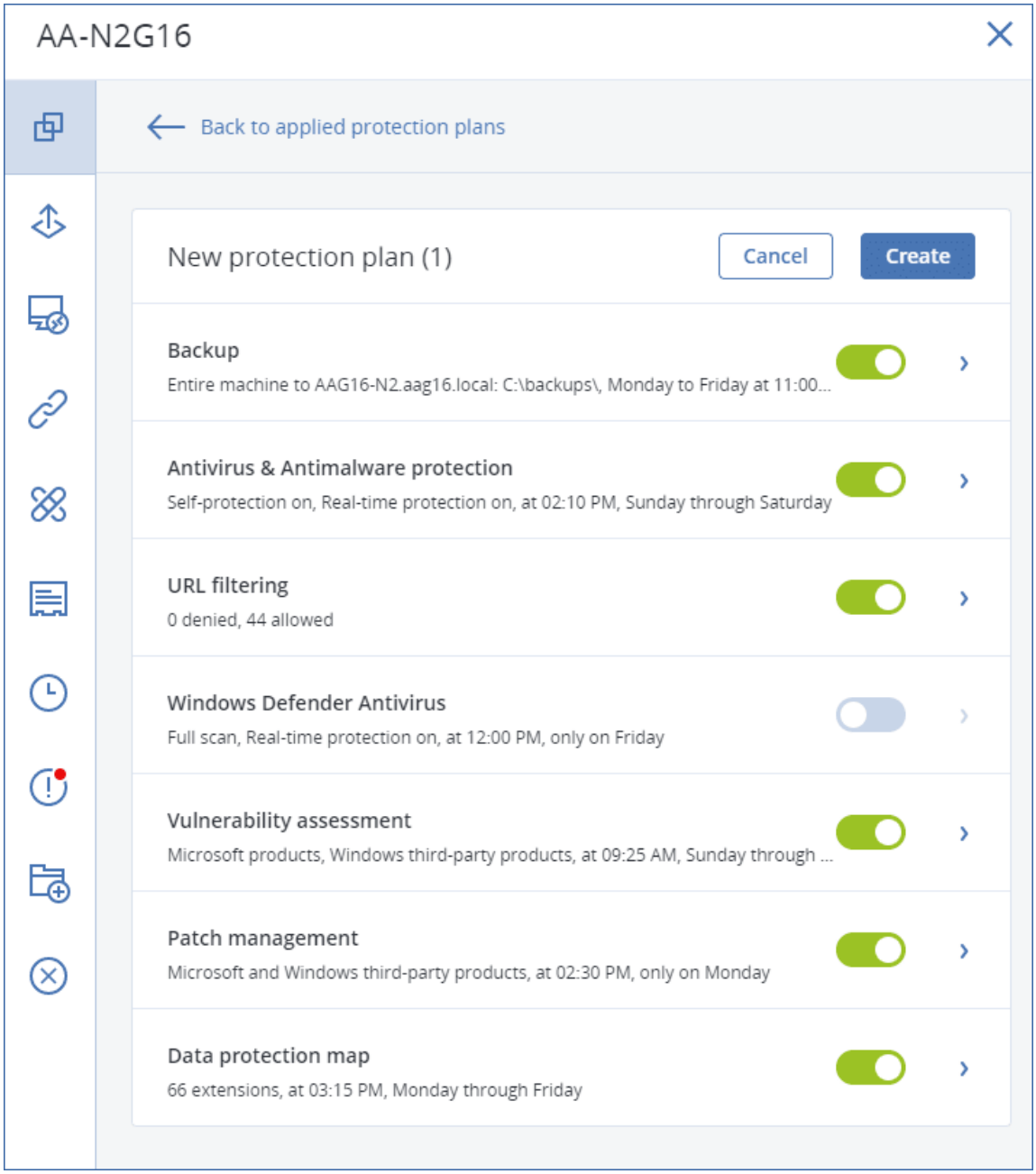
Розглянемо перший спосіб.

Щоб створити перший план захисту необхідно:

1. У веб-консолі Cyber Protect перейдіть до Пристрої > Усі пристрої .

2. Виберати машини, які ви хочете захистити.

Натисніть «Захистити» , а потім — «Створити план». Тепер буде видно план захисту з параметрами за замовчуванням (рис 3.2).



3.2. План захисту

Крім цьогоможна змінити назву плану захисту, увімкнути або вимкнути модуль плану захисту, налаштувати параметри модуля. Коли все буде зроблено - натисніть «Створити».

3.3. Загадьні рекомендації щодо використання Acronis Cyber Protect

Acronis Cyber Protect — це комплексне рішення для кібербезпеки, яке пропонує ряд функцій, включаючи резервне копіювання, захист від зловмисного програмного забезпечення, керування виправленнями та аварійне відновлення. Ось кілька загальних рекомендацій щодо використання Acronis Cyber Protect:

Плануйте та розкладайте резервне копіювання. Однією з ключових особливостей Acronis Cyber Protect є функція резервного копіювання. Важливо спланувати та запланувати регулярне резервне копіювання важливих даних, щоб гарантувати їх відновлення у разі втрати даних.

Підтримуйте своє програмне забезпечення в актуальному стані: Acronis Cyber Protect пропонує функції керування виправленнями, які допоможуть вам підтримувати актуальне та безпечне програмне забезпечення. Переконайтеся, що ви регулярно оновлюєте програмне забезпечення до останніх версій і застосовуєте виправлення безпеки, щойно вони стануть доступними.

Налаштуйте параметри захисту від зловмисного програмного забезпечення: Acronis Cyber Protect включає функції захисту від зловмисного програмного забезпечення, які можуть допомогти захистити ваші системи від зараження шкідливим програмним забезпеченням. Налаштуйте параметри захисту від зловмисного програмного забезпечення відповідно до ваших потреб і заплануйте регулярне сканування.

Слідкуйте за своїми системами: стежте за своїми системами, щоб виявити будь-яку незвичайну активність або аномалії, які можуть свідчити про порушення безпеки. Використовуйте функції моніторингу та звітування в Acronis Cyber Protect, щоб допомогти вам визначити потенційні загрози.

Навчіть своїх співробітників: навчіть своїх співробітників передовим практикам кібербезпеки, наприклад, створюйте надійні паролі, уникайте підозрілих електронних листів і не натискайте посилання з невідомих джерел. Це допоможе знизити ризик кібератак.

Перевірте свій план аварійного відновлення: Acronis Cyber Protect пропонує функції аварійного відновлення, які можуть допомогти вам відновити роботу після аварії. Регулярно тестуйте свій план аварійного відновлення, щоб переконатися, що він працює належним чином і що ви можете швидко й ефективно відновити свої дані.

Acronis Cyber Protect включає кілька функцій для захисту від зловмисного програмного забезпечення, наприклад захист від зловмисного програмного забезпечення та оцінку вразливості. Ось кілька способів використання Acronis Cyber Protect для захисту від шкідливих програм:

Увімкніть захист від зловмисного програмного забезпечення: Acronis Cyber Protect включає захист від зловмисного програмного забезпечення, який може виявити та видалити зловмисне програмне забезпечення з ваших систем. Переконайтеся, що захист від шкідливих програм увімкнено та налаштовано на автоматичне регулярне сканування ваших систем.

Налаштуйте параметри захисту від зловмисного програмного забезпечення: налаштуйте параметри захисту від зловмисного програмного забезпечення відповідно до ваших конкретних потреб, як-от планування регулярних сканувань, налаштування захисту в режимі реального часу та створення списків виключень для довірених програм.

Виконайте оцінку вразливості: Acronis Cyber Protect містить функції оцінки вразливості, які можуть виявити потенційні слабкі місця безпеки у ваших системах. Використовуйте ці функції, щоб регулярно сканувати свої системи та виправляти виявлені вразливості.

Оновлюйте програмне забезпечення: оновлюйте програмне забезпечення за допомогою останніх виправлень і оновлень безпеки. Acronis Cyber Protect включає функції керування виправленнями, які можуть допомогти вам керувати оновленнями програмного забезпечення та гарантувати, що ваші системи захищені від відомих уразливостей.

Регулярне резервне копіювання: окрім захисту від зловмисного програмного забезпечення, також важливо мати план резервного копіювання, щоб забезпечити можливість відновлення даних у разі атаки зловмисного програмного забезпечення. Acronis Cyber Protect містить функції резервного копіювання, які допоможуть безпечно створити резервну копію та відновити ваші дані.

Використання Acronis Cyber Protect захистить корпоративне середовище від кіберзагроз. Дотримуючись цих загальних рекомендацій, дозволить отримати максимальну користь від програмного забезпечення та зменшити ризик кібератак.

ВИСНОВКИ

В результаті виконання бакалаврської роботи було отримано наступні результати:

Проаналізовона поняття корпоративного середовища та їх структуру. В результаті якого отримано розуміння як циркулює інформація в організації на снові клієнт-серверної архітектури.

Отримано статистику впливу загроз від шкідливих програм в корпоративному середовищі організацій, в результаті якого визначено необхідність впровадження заходів щодо захисту від шкідливих програм.

Проведено порівняння рішень з захисту від шкідливого програмного забезпечення. Кожне з розглянутих рішень є комплексним рішенням, яке включає в себе різні методи та засоби. Для подальшого дослідження було обрано рішення Acronis Cyber Protect, яке містить функції резервного копіювання, що дозволяє швидше відновити роботу від впливу шкідливих програм.

Досліджено методи та засоби захисту від шкідливого програмного забезпечення корпоративного середовища на основі архітектури та основних функцій рішення Acronis Cyber Protect.

Розроблено рекомендації щодо роботи модуля «Антивірус та захист від шкідливих програм» дозволяє захистити машини Windows та macOS від усіх нових загроз з боку шкідливих програм та надано загальні рекомендації фахівціям з кібербезпеки щодо захисту від шкідливих програм.

ПЕРЕЛІК ПОСИЛАНЬ

1. Корпоративне середовище [Електронний ресурс] Режим доступу: https://www.investopedia.com/terms/o/organizational-structure.asp.

2. Клієнт-серверна архітектура [Електронний ресурс] Режим доступу: https://www.interviewbit.com/blog/client-server-architecture/.

3. Шкідливе програмне забезпечення [Електронний ресурс] Режим доступу: https://www.myrasecurity.com/en/malware/.

4 Рейтинг загроз [Електронний ресурс] Режим доступу: https://www.comparitech.com/antivirus/malware-statistics-facts/

5 Захист робочих станцій [Електронний ресурс] Режим доступу: https://www.eset.com/ua/business/solutions/endpoint-protection/.

6 ESET Endpoint [Електронний ресурс] Режим доступу: https://www.eset.com/fileadmin/ESET/INT/Products/Business/Endpoint/Endpoint/EES-Windows/v09/ESET_Endpoint_Solutions_Product_Overview.pdf.

7. Найкращі програми безпеки [Електронний ресурс] Режим доступу: https://techukraine.net/6-найкращих-програм-безпеки-в-інтернет/#Авіра_Прайм.

8. Acronis Cyber Protect [Електронний ресурс] Режим доступу: https://www.acronis.com/en-us/products/cyber-protect/?utm_medium=affiliate&utm_source=8517397&utm_campaign=cj&utm_content=14491575&utm_term=&cjevent=866c429bd90511ed825d79480a18b8fc

9. Acronis Cyber Protect. Посібник. - 2022. 101с.

10. Acronis Ransomware Protection. Guide. – 2017. 27с.

КОПІЇ ДЕМОНСТРАЦІЙНИХ АРКУШІВ