УДК 004.056.5 **doi: 10.26906/SUNZ.2023.4.102**

Д. В. Сердюков, О. В. Сєвєрінов, З. М. Сидоренко

Харківський національний університет радіоелектроніки, Харків, Україна

ОСОБЛИВОСТІ РОЗГОРТАННЯ ЗАСТОСУНКУ ESET MDM/MDC ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

Анотація. Предметом дослідження в статті є аналіз можливостей та процесу розгортання застосунку ESET Mobile Device Connector (MDC) з метою забезпечення безпеки та управління мобільними пристроями в корпоративних середовищах. В статті вирішуються наступні **завдання**: розгляд структури та складових функцій MDC системи, визначення основних проблем та недоліків під час активації продукту та конфігуруванні системи.. Отримано наступні результати: розглянута структура роботи системи MDC, порядок її розгортання, виявлено недоліки під час інсталяції та способи їх вирішення, заблоковано загрози системою MDM . **Висновки**: Дослідження підтвердило, що встановлені політики та система MDM ефективно заблоковують вразливості та загрози на мобільних пристроях в корпоративних мережах, але вимагають правильних налаштувань та досвіду для успішного розгортання.

Ключові слова: MDM система, MDC система, віддалене керування мобільними пристроями, захист корпоративної інформації, СУІБ.

Вступ

Постановка проблеми. Відомо, що мобільні пристрої принесли багато користі організаціям у вигляді підвищення мобільності, доступу до інформації та зручності в роботі.

В любому випадку співробітник за допомогою смартфону отримує доступ до інформації що обробляється в організації, починаючи від фотографій та клієнтів електронної пошти, закінчуючи застосунками з одноразовими ключами для двофакторної автентифікації.

Однак їхнє використання також вимагає ретельного планування і управління, щоб забезпечити безпеку та ефективність бізнес-процесів.

Крім того, користувачі мобільних пристроїв часто мають можливість пропускати оновлення додатків та операційної системи, встановлювати сторонні програми та підключатися до особистих і загальнодоступних мереж Wi-Fi. Хоча ці функції і допомагають користувачам, вони піддають дані на цих пристроях серйозному ризику витоку або крадіжки зловмисниками.

Ці вразливості безпеки стають більш тривожними, коли співробітники використовують власні смартфони, планшети та ноутбуки для доступу та обміну ІзОД не попереджуючи відділ інформаційної безпеки організації.

Одне порушення призводить до того, що організація не дотримується державних стандартів, нормативних документів і сплачує великі штрафи при першій же перевірці. Якщо, звісно, компанія не проводить внутрішній або зовнішній аудит інформаційної безпеки хоча б раз на рік та не виявляє дані порушення в ручному режимі [1].

Тому, для забезпечення захисту інформації, контролю встановлених застосунків, керування антивірусними системами та методами вводу, виводу інформації, використовують сервіси Mobile Device Management (далі - MDM).

Метою даного дослідження є аналіз можливостей та процесу розгортання застосунку ESET MDM/MDC для забезпечення безпеки мобільних пристроїв в корпоративних середовищах.

Виклад основного матеріалу

Структурна схема роботи MDC. Mobile Device Connector (далі - MDC) – це частина ієрархії ESET PROTECT, яка забезпечує зв'язок між мобільними пристроями та самого веб-серверу ESET для використання функцій MDM. MDM – системи повного контролю за мобільними пристроями, Device Loss Prevention та Mobile Application Management є невід'ємною його частиною [2, 3].

На рис. 1 наведено структурну схему обміну даними між продуктами ESET PROTECT та мобільними пристроями [2].

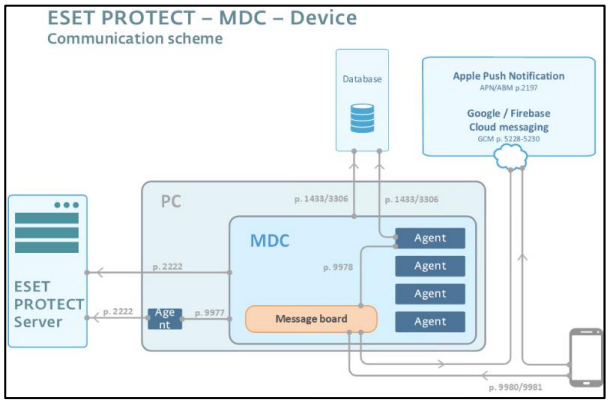

Рис. 1. Структурна схема роботи MDC

MDC – це рішення яке дозволяє керувати мобільним пристроями без агентів. Для збереження ресурсів мобільних пристроїв, агенти не працюють на самих пристроях.

Сервіс є хостом з віртуальними агентами. Дані для керування пристроями зберігаються у БД SQL. Сертифікат HTTPS необхідний для автентифікації обміну даними між мобільним пристроєм і MDC. Сертифікат проксі-сервера використовується для автентифікації зв'язку між сервером ESET PROTECT та MDC [2].

До керування пристроями Apple застосовуються додаткові вимоги, такі як спеціалізовані сертифікати, які необхідно підписувати довіреними центрами сертифікації Apple. На відміну від Apple, пристрої на

основі ОС Android не мають спеціальних умов до сертифікатів [4]. Через це переведення таких пристроїв на керування є простішим та займає менше часу.

Аналіз реагування системи MDM. Для аналізу реагування на вразливості, що виникають на мобільних пристроях підключених до мережі, були додані стандартні політики:

- міжмережевий екран;
- веб-захист;
- антивірус.

Всі вони спираються на існуючі правила і списки, які надає та оновлює в реальному часі репозиторій ESET. Ці правила і списки, можна створювати самостійно. В результаті проведених досліджень були отримані результати, що наведені на графіку реагування згідно встановленим політикам за період в 7 днів на 5 мобільних пристроях (рис. 2).

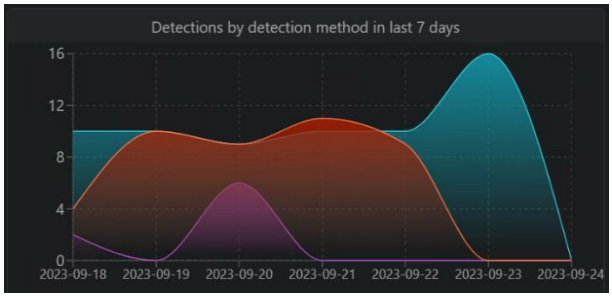

Рис. 2. Графік кількості заблокованих вразливостей за тиждень. (Фіолетовий – Антивірусних захист, Червоний – Веб-захист, Блакитний – міжмережевий екран)

На рис.3 можна переглянути результати дослідження кількості виявлених і заблокованих спроб порушення встановлених правил на мобільних пристроях за 31 день.

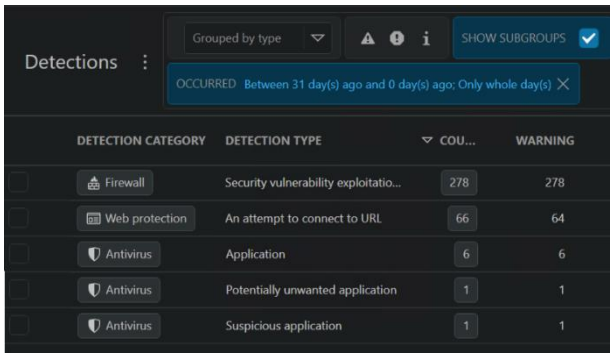

Рис. 3. Статистика виявлення з сортуванням за категорією правил

НСД, спроби доступу на небезпечні URL-адреси, потенційно небажані та підозрілі застосунки, експлуатація вразливостей були успішно заблоковані встановленими політиками на мобільних пристроях.

Але розгорнути ESET MDC адміністратору, який не мав досвіду з подібними сервісами, не так просто. При дослідженні були розроблені рекомендації щодо встановлення сервісу на Windows Server 2016 та підключення його до Веб-додатку. Далі розглянемо кроки інсталяції.

Основні кроки інсталяції MDC. В консолі ESET PROTECT отримуємо посилання до офіційного репозицію, звідки можна завантажити інсталятор. Запускаємо інсталятор, ознайомлюємось з Ліцензійною угодою користувача та приймаємо її.

Далі необхідно підкріпити HTTPS сертифікат підписаний власним центром сертифікації ESMS Certification Authorities. Для цього потрібно відкрити веб-застосунок ESET Protect, в меню Certification Authorities згенерувати сертифікат Агента (рис. 4).

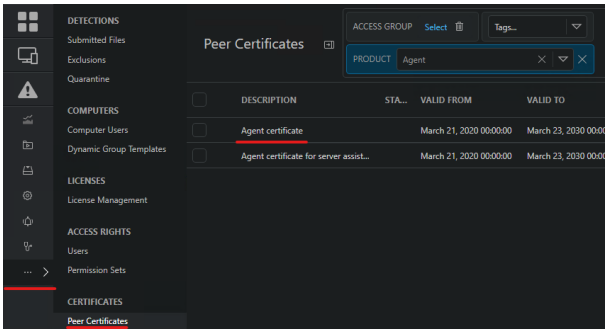

Рис. 4. Згенерований сертифікат

Прикріплюємо сертифікат до інсталяції. В наступному кроці адміністратори зазвичай стискаються з проблемою. Після першого налаштування основного серверу ESET Protect, який може налаштовувати інший адміністратор, рекомендується змінити стандартні порти доступу до БД. Новий адміністратор, що розгортає MDC пробує підключитись до бази даних по стандартному порту і не отримує доступу. Саме тому рекомендується розгортати MDC на тій самій БД що й ESET Protect. era_db – стандартна назва БД, а 1433 – стандартний порт підключення до неї. Замість цього, вам потрібно створити окрему базу даних під назвою era_mdb поруч з основною era_db, створити окремого адміністратора для цієї бази даних і змінити порт за замовчуванням для цієї нової бази даних. Також, необхідно замінити налаштування localhost на ім'я серверу куди встановлюється конектор, тобто, сервер ESET Protect.

Отже, ці заходи забезпечують безпеку та оптимізацію роботи системи ESET Protect та бази даних MDC.

На рис. 5 та 6 представлені налаштування за-замовчуванням – перший та бажані – другий.

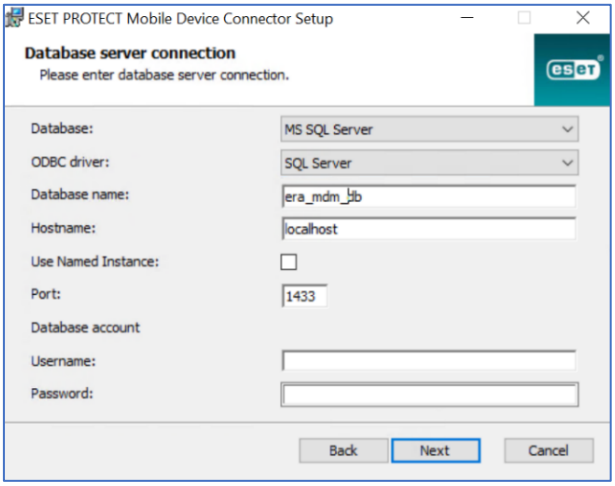

Рис. 5. Налаштування за-замовчуванням

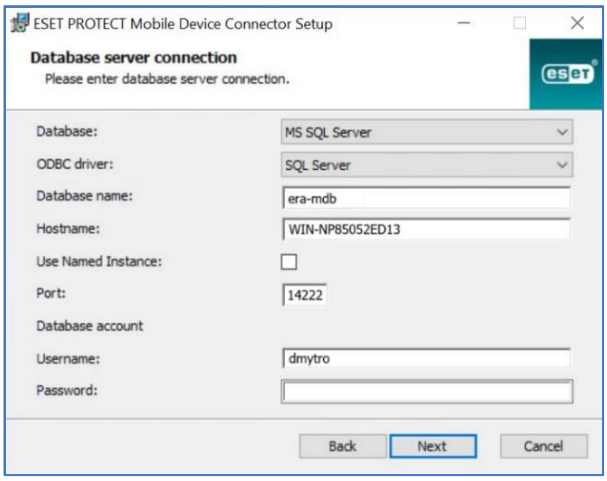

Рис. 6. Налаштування підключення до БД

Наступним кроком підключення до веб-серверу, порти залишаємо без змін, замінюємо server host відповідно до назви серверу організації (рис. 7).

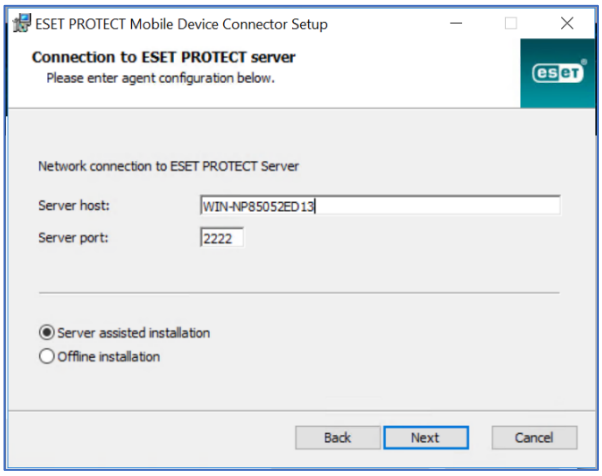

Рис. 7. Підключення до веб-серверу

На фінальному кроці треба надати облікові дані для підключення до веб-серверу. Проведені дослідження виявили, що облікові дані, на яких налаштовано двофакторну автентифікацію, не підтримуються (рис. 8). Виробник програмного забезпечення рекомендує одразу включати її після створення аккаунту.

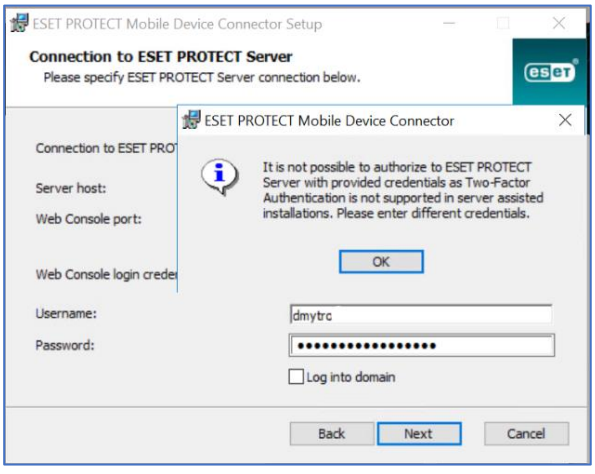

Рис. 8. Помилка під час доступу до серверу

Для подальшої інсталяції необхідно створити обліковий запис користувача для реєстрації на сервері. Права доступу обов'язково повинні буди Адміністративні. Заходимо на веб-сервер, в даному випадку https://WIN-NP85052ED13/era/# id=USERS, відкриваємо меню **Користувачі** та створюємо нового користувача **mdmuser** з Наборами дозволів **Administration permission set** без двофакторної автентифікації. Використовуючи нові облікові дані, маємо фінальний крок та підтверджуємо місце інсталяції застосунку. Після чого почнеться процес інсталяції (рис. 9). Після успішної інсталяції можна відкрити консоль віддаленого адміністрування. Переглянути сповіщення про стан системи (рис. 10).

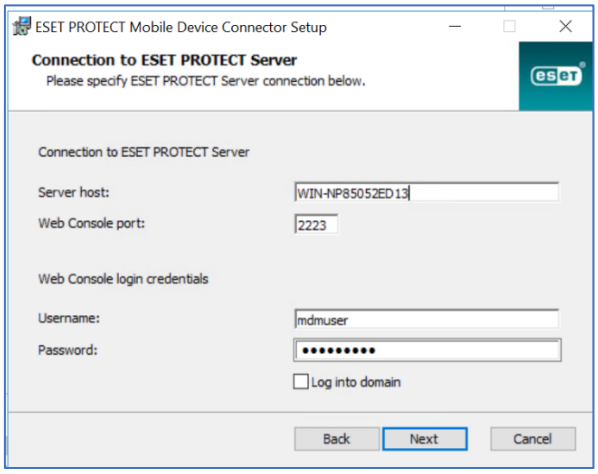

Рис. 9. Конфігурація підключення до веб-серверу та місця інсталяції

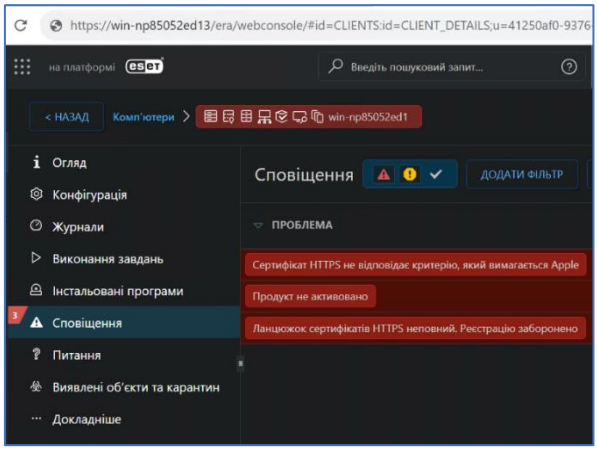

Рис. 10. Важливі сповіщення системи безпеки

Обов'язковою вимогою є активація продукту, окрема ліцензія не використовується, тільки основна, якою активовані інші продукти на даному сервері. Ліцензії купують на робочі станції або користувачів, їх можна перезначати на інші станції, уразі виходу з ладу або заміни. Тому купувати ліцензії з запасом не обов'язково, завжди можна докупити робочі місця або користувачів.

Перед реєстрацією мобільних пристроїв необхідно згенерувати сертифікати, що будуть відповідати критеріям Apple. Та доповнити ланцюжок сертифікатів HTTPS [5].

За даним методом інсталяції можна використовувати різні сертифікати: якщо організація має центр сертифікації, генерує та використовує власні сертифікати для веб-серверів, то даний сервіс підтримує використання сторонніх сертифікатів HTTPS. Але для пристроїв Apple, обов'язково, повинні бути створені сертифікати APN/ABM та підписані довіреним центром сертифікації Apple [5]. ESET має власний центр сертифікації ESET PROTECT, який може генерувати сертифікати однорангових вузлів для агентів [6].

VPN – тунелювання. Однією з ключових складових мобільної безпеки є забезпечення безпечного з'єднання між мобільними пристроями та серверами організації. У цьому контексті, використання віртуальної приватної мережі (VPN) виявляється дієвим інструментом для забезпечення захищеного зв'язку, який дозволяє уникнути можливих атак і перехоплення даних [7]. Завдяки використанню VPN, адміністратори можуть забезпечити безпеку та конфіденційність даних, що передаються між мобільними пристроями та серверами MDC [6]. VPN дозволяє створити захищене тунельне з'єднання, шифруючи дані та захищаючи їх від несанкціонованого доступу. Це особливо важливо в сферах, де зберігаються чутливі корпоративні дані, такі як персональні дані клієнтів, фінансові дані та інтелектуальна власність. Тому обов'язковою вимогою є підключення керованих мобільних пристроїв до корпоративної мережі та центру керування пристроями тільки через захищене тунельне з'єднання [7].

Додавання VPN до арсеналу заходів забезпечення безпеки в MDC підвищує рівень надійності та довіри до системи управління мобільними пристроями. Захищений зв'язок сприяє попередженню можливих атак і забезпечує безпеку даних під час їх передачі. Окремі системи також можуть використовувати автентифікацію при доступі до корпоративної мережі шифрування усього трафіку. Присутня можливість створювати для кожного додатка окремий VPN канал, що також забезпечує додаткову захищеність за умови використання загальнодоступних або ненадійних мереж [7].

Висновки

У статті було розглянуто питання розгортання застосунку ESET Mobile Device Connector (MDC) для забезпечення безпеки та управління мобільними пристроями в корпоративних середовищах. Дослідження показало, що ефективне розгортання MDC може значно підвищити рівень безпеки та продуктивності в організаціях, де мобільні пристрої використовуються для роботи та обміну даними. За допомогою правильних налаштувань та практичних кроків, адміністратори можуть успішно розгортати MDC, забезпечуючи відповідність стандартам безпеки та вимогам корпоративних нормативних документів. Важливими етапами є створення окремої бази даних для MDC, налаштування серверу та веб-серверу, а також генерація сертифікатів, що відповідають критеріям Apple. Додатково, активація продукту та належна конфігурація системи є важливими кроками для успішної роботи MDC. Організації повинні також враховувати можливість докупівлі ліцензій в разі необхідності розширення обсягу захисту мобільних пристроїв. Загалом, розгортання MDC може бути ефективним інструментом для управління мобільною безпекою та підвищення продуктивності в сучасних корпоративних середовищах. Важливо дотримуватися найкращих практик та забезпечувати відповідність стандартам безпеки для досягнення успішних результатів.

Список літератури

1. Why VPNs on mobile devices are a crucial part of securing access to corporate data - ManageEngine Blog. ManageEngine Blog. [Електронний ресурс]:[Веб-сайт]-Режим доступу: https://cutt.ly/V41SZjN
2. MDM Setup and Settings Режим доступу: https://help.eset.com/protect_admin/10.0/en-US/mdm_setup_and_settings.html
3. Нечволод К.В., Сєвєрінов О.В., Власов А.В. Аналіз безпеки даних в EMM системах / Системи управління, навігації та зв'язку. Збірник наукових праць 3.55 (2019): 131-134.
4. Нечволод, К.В., Сєвєрінов О.В. Аналіз захищеності системи Android для використання в корпоративному сегменті. 2019.
5. Обмеження MDM для пристроїв iPhone та iPad [Електронний ресурс]:[Веб-сайт]-Режим доступу: https://support.apple.com/uk-ua/guide/deployment/dep0f7dd3d8/web (дата доступу: 24.09.2023).
6. Best Mobile Device Management (MDM) Software [Електронний ресурс]:[Веб-сайт]-Режим доступу: https://www.g2.com/categories/mobile-device-management-mdm (дата доступу: 24.09.2023).
7. Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. – Том 1, 70 (2023).

Received (Надійшла) 15.09.2023
Accepted for publication (Прийнята до друку) 22.11.2023

Deployment features of ESET MDM/MDC application for mobile device security

D. Serdiukov, O. Sievierinov, Z. Sydorenko

Abstract. The article focuses on the analysis of capabilities and the deployment process of the ESET Mobile Device Connector (MDC) application with the aim of ensuring security and mobile device management in corporate environments. **The following tasks are addressed in the article**: an examination of the structure and components of the MDC system's functions, identification of key issues and drawbacks during product activation and system configuration. **The following results have been obtained**: the working structure of the MDC system is reviewed, the deployment process is outlined, installation issues are identified, and methods to address them are discussed. The MDM system effectively mitigates threats to mobile devices within corporate networks, although it requires proper configuration and experience for successful deployment.

Keywords: MDM system, MDC system, remote mobile device management, corporate information protection, ISMS.