ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Богдан МЕНЧИНСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
МЕНЧИНСЬКИЙ Богдан
(прізвище, ім'я)

Керівник к.т.н., доцент ВЛАСЕНКО Вадим
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ВСТУП

Актуальність дослідження. У наш час використання смартфонів, планшетів, ноутбуків стало невід'ємною частиною робочого графіка більшості організацій і корпорацій. Багато з них ухвалюють нову політику, яка дозволяє працівникам використовувати власні пристрої на робочому місці. Незважаючи на економічні переваги та переваги використання, політика Bring Your Own Device може створити серйозні ризики безпеці та мати негативний вплив залежно від етики працівників і відсутності гарантій у компанії. Комп'ютерним адміністраторам тепер потрібно керувати кількома різними обліковими записами користувачів на різних веб-сайтах, серверах, комп'ютерах і мобільних пристроях. Щоб адміністратори могли контролювати свої комп'ютерні системи, вони повинні почати використовувати програмне забезпечення, яке допомагає контролювати всі облікові записи користувачів і пристрої в одному місці.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження технології управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD.

Об'єкт дослідження – управління мобільними користувачів корпоративної інформаційної системи з використанням концепції BYOD.

Предмет дослідження – технологія управління захистом мобільних користувачів корпоративної інформаційної системи з використанням концепції BYOD на прикладі рішення Unified Endpoint Management.

Мета роботи – дослідити технологію управління мобільними користувачами корпоративної інформаційної системи на основі концепції BYOD та розробити варіант управління їх захистом на підприємстві.

Наукові завдання:

дослідити сутність проблеми управління користувачами політики BYOD на корпоративну інформаційну мережу;

встановити ризики безпеки при створенні системи безпеки за концепцією BYOD;

проаналізувати існуючі методи та засоби управління мобільними користувачами концепції BYOD;

проаналізувати основні функції та принципи управління мобільними користувачами концепції BYOD.

розробити варіант управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD та розробити рекомендацій щодо технології управління мобільними користувачами корпоративної інформаційної системи для фахівців а кібербезпеки.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи захисту корпоративних мобільних пристроїв.

Практичне значення одержаних результатів полягає в розробці варіанта управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD, а також у розробці рекомендацій технології управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD.

Апробація результатів кваліфікаційної роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка

відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ МОБІЛЬНИМИ КОРИСТУВАЧАМИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ З ВИКОРИСТАННЯМ КОНЦЕПЦІЇ BYOD

1.1. Аналіз політики BYOD на корпоративну інформаційну мережу

Bring Your Own Device (BYOD) — це використання персональних мобільних пристроїв, таких як ноутбуки, планшети та смартфони, для доступу до мереж, систем і конфіденційної інформації компанії в організації. BYODs стали поширеними на робочому місці через збільшення залежності від Інтернету та прогресу в технологіях [1].

BYOD пропонує працівникам комфорт їхніх власних пристроїв, більше простоти у використанні та дозволяє налаштовувати пристрої відповідно до індивідуальних потреб Дослідники виявили, що головною перевагою використання BYOD є продуктивність, оскільки організації можуть заощадити тисячі на витратах на інформаційні технології (IT) шляхом впровадження стратегії BYOD, зниження вартості оренди пристроїв і витрат на управління для розгортання, фіксування витрат на підтримку та страхування, уникаючи щорічних оновлень пристроїв, що належать компанії [6].

Кожного разу, коли персональні пристрої взаємодіють із корпоративною мережею, існує ризик втрати даних і зламу, і, на жаль, потенційні ризики безпеки щодо конфіденційності існують для багатьох організацій, що створює проблеми для безпеки інформаційних систем. Безпека інформаційних систем передбачає захист інформації та інформаційних систем від несанкціонованого доступу або модифікації інформації під час зберігання, обробки чи передачі, а також від відмови в обслуговуванні авторизованих користувачів. Це означає, що використання BYOD у неконтрольованому середовищі посилює вплив інформації компанії та інформаційних систем. Зокрема фінансові установи обробляють дуже конфіденційну інформацію, що робить їх мішенню для витоку даних і застосування BYOD є більш небезпечним. Ризики, пов’язані з порушенням безпеки, можуть мати негативний вплив на фінансові установи, що може завдати шкоди їхній репутації,

прибутковості та навіть призвести до закриття бізнесу. За даними Insights (2023), 25,7 відсотка всіх атак зловмисного програмного забезпечення були спрямовані на фінансові установи. Thielens (2023) зауважив, що критичною проблемою BYOD є контроль доступу з пристроїв до даних організації. Таким чином, при застосуванні політики безпеки BYOD слід враховувати такі аспекти, як контроль доступу, виявлення вторгнень, криптографія, безпека пристрою та управління безпекою.

Важливо розуміти, як BYOD можуть негативно вплинути на стратегію безпеки інформаційних систем фірми. Узгодження BYOD з політикою інформаційної безпеки фірми допомагає менеджерам визначити, що дозволено робити працівнику під час доступу до мережі компанії. Важливо мати програму, яка заохочуватиме працівників бути поінформованими про їхні зобов'язання щодо інформаційних активів фірми [5].

Chigada and Kyobe (2018) встановили, що інсайдерські атаки та випадкова публікація конфіденційної інформації співробітниками мають найбільший вплив на безпеку, поступаючись хакерським атакам у успішному зламуванні їхніх організацій. Хоча фірми стурбовані забезпеченням безпеки, працівники стурбовані збереженням практичності своїх пристроїв і конфіденційністю своєї особистої інформації. Проблеми, які виникають у зв'язку з дотриманням політики безпеки, полягають у тому, що працівники можуть відчувати, що існують перешкоди для використання їхніх пристроїв, наприклад, вони не знайомі з інстальованим програмним забезпеченням безпеки, яке може обмежувати доступ до їхнього пристрою. Незважаючи на широке впровадження ініціативи BYOD у секторі фінансових послуг, багатьом організаціям все ще бракує розуміння ризиків, пов'язаних з BYOD під час підключення до їхніх мереж, і не вживають достатніх заходів безпеки для боротьби з цими проблемами безпеки.

Тенденція BYOD набуває популярності в усіх галузях промисловості, і зокрема сектор фінансових послуг отримав широке впровадження BYOD. BCG (2020) виявив, що індустрія фінансових послуг у 300 разів більш сприйнятлива до порушень безпеки та атак, ніж будь-яка інша галузь, через характер цих підприємств і конфіденційні дані, які вони обробляють. Відсутність належного

захисту та збільшення BYOD в їхніх організаціях ще більше ускладнюють виявлення та запобігання витоку інформації. Таким чином, практика управління інформаційною безпекою має бути надзвичайно важливою у фінансовому секторі, щоб захистити конфіденційну інформацію компанії [8].

Використання персональних пристроїв з'явилося ще в 2003 році, але концепція BYOD почала набирати популярності в 2011 році, в основному завдяки напливу розумних мобільних пристроїв разом із експоненційним зростанням підключення до Інтернету. Споживання IT розширює можливості використання BYOD, і організації зрозуміли, що BYOD не можна ігнорувати. BYOD надають організаціям конкурентну перевагу, тому їх слід включити до їхньої IT-стратегії, якщо вони хочуть залишатися актуальними в цифрову еру (Chenget al., 2023). Розумні пристрої є доступними та дозволяють користувачам працювати практично з будь-якого місця, значно підвищуючи гнучкість до доступу. Співробітники можуть працювати швидше завдяки знайомству зі своїми пристроями, створюючи сплеск продуктивності, що є однією з головних причин впровадження BYOD. Frost & Sullivan (2021) повідомили, що продуктивність підвищилася на 34 відсотки за використання персональних пристроїв і заощадила співробітникам 58 вільних хвилин на день порівняно з тими, хто не використовував BYOD.

Musarurwa та ін. (2022) стверджують, що BYOD відволікають увагу, оскільки працівники також мають доступ до розваг, приймають особисті дзвінки та переглядають соціальні мережі в робочий час, що є контрпродуктивним. BYOD можна використовувати як ініціативу з економії коштів, зменшуючи витрати на апаратне забезпечення, знижуючи витрати на обслуговування пристроїв і знижуючи витрати на страхування для організацій (Insights, 2023). Kaneshige (2022) стверджує, що компанії можуть думати, що вони економлять на витратах на мобільні пристрої, але існують витрати на безпеку та відповідність, які не завжди враховуються [3].

1.2. Ризики безпеки, спричинені BYOD

Хоча BYOD приносять переваги працівникам і бізнесу, вони також створюють численні проблеми для організацій. BYOD підключаються до точок доступу до мережі на робочому місці, що відкриває організації для потенційних атак, які проникають через пристрої. Оскільки пристрої є приватною власністю, IT стикається з проблемою, як захистити свої інформаційні активи та конфіденційні дані від злому, втрати чи неналежного використання [7].

Викрадення даних.

Безпека даних порушується, коли пристрої втрачаються або викрадаються. За даними EY (2021), дедалі більше пристроїв, які були втрачені та викрадені, вміст переглядав хтось інший. Оскільки BYOD можуть містити конфіденційні дані компанії, вони відкривають двері для порушників, щоб отримати доступ до цієї інформації.

Атаки з впровадження зловмисного програмного забезпечення.

Компанії дедалі частіше страждають від зловмисного програмного забезпечення, створеного з метою пошкодження пристроїв, крадіжки інформації та навіть можуть використовуватися для контролю пристроїв. Зловмисне програмне забезпечення може бути закодовано в програмах, встановлених на пристроях, або виявлено, коли користувач відвідує скомпрометований веб-сайт. Прикладом є банківський троян Carbanak, якому вдалося проникнути у фінансові установи у 2013 році. Зловмисне програмне забезпечення проникло в організації, спонукаючи працівників натискати шкідливі електронні листи, що забезпечувало канал для переміщення зловмисників через корпоративну мережу для дистанційного керування банкоматами, також відомого як «джекпотінг». Група Fin7, яка використовує Carbanak, за останні три роки вкрала понад 1 мільярд євро з банків у понад 40 країнах і атакувала понад 120 американських компаній (Європол, 2020).

Інсайдери.

Інсайдери зловживають своїми повноваженнями та знаннями про організацію, щоб отримати доступ до конфіденційних даних, інформації та інших

цінних активів для власної корисливої вигоди. Завдяки BYOD це стало ще більшим ризиком через технічні можливості пристрою.

Shadow IT.

BYOD спричинив використання тіньових IT, використання пов'язаних з IT хмарних служб, апаратного забезпечення чи програм без відома IT-відділу чи відділу безпеки організації. Зростання тіньових IT значною мірою пов'язано з тим, що співробітники хочуть працювати ефективніше та обійти недоліки інформаційних систем, розгорнутих в організаціях. Згідно з Chejfec (2020), лише дві третини IT-менеджерів визнають тіньові IT як існуюче явище в їхній організації, оскільки співробітники та бізнес використовують ці IT-ресурси автономно для підтримки своїх процесів. Тіньові IT ускладнюють для IT-відділів відстеження, керування, підтримку та захист IT-інфраструктури на робочому місці, оскільки організації не знають про пристрої, підключені до їхніх мереж, і навіть якщо вони знають, не існує політики для контролю.

Відсутність політик BYOD.

Керування особистими пристроями співробітників не є простим завданням і, на жаль, у більшості організацій не обробляється належним чином. За даними Kearns (2020) і Investopedia (2020), більшість організацій не змогли вирішити проблеми безпеки за допомогою формальних політик і створити засоби контролю, щоб мінімізувати їх виникнення. Gustav and Kabanda (2020) встановили, що численні організації, які мали відповідні ресурси в інфраструктурі, все ще не змогли формалізувати стратегію BYOD, незважаючи на її використання. Відсутність політики BYOD означає, що співробітники не навчені тому, як відповідально, ефективно та належно використовувати персональні технології для роботи, що могло б взагалі уникнути багатьох проблем безпеки. Для організацій стає постійним викликом моніторинг та оновлення політики BYOD, оскільки технології та законодавчі закони, що стосуються рівня контролю організацій, постійно розвиваються. Хоча багато організацій запроваджують політику безпеки для запобігання ризикам безпеки BYOD, працівники часто ігнорують її. Інші проблеми, які виникають, полягають у тому, що працівники не знають про існуючу

політику BYOD або забувають про те, що політику BYOD їм було представлено. Зважаючи на постійні випадки промислового шпигунства та витоку інформації в організаціях, очевидно, що потрібне суворе застосування політики BYOD. Якщо політики не дотримуються, вони втрачають свою ефективність.

Неефективні механізми контролю безпеки та видимості

Механізми безпеки мобільних пристроїв включають шифрування, автентифікацію, можливості віддаленого стирання, гарячі лінії втрачених телефонів, брандмауери, використання стороннього програмного забезпечення, програмне забезпечення для запобігання вторгненню та антивірусне програмне забезпечення. На жаль, зростання можливостей і продуктивності мобільних пристроїв спричинило сплеск проблем із безпекою та існуючих механізмів безпеки, які не завжди адаптовані до нових технологій. Більшість мобільних пристроїв не мають розширених функцій безпеки, а співробітники навіть відключають існуючі базові функції, такі як керування паролями. IT-відділи погано поінформовані про те, чи встановлено чи оновлено антивірусне програмне забезпечення на пристрої співробітників. Відсутність механізмів контролю безпеки на пристроях співробітників може призвести до відсутності контролю над даними компанії, що призведе до витоку даних і наслідків, пов’язаних з крадіжкою даних.

Відсутність обізнаності про безпеку.

Обізнаність про безпеку визначається як ставлення та знання представника організації щодо захисту інформаційних активів своєї організації. Заходи з підвищення обізнаності про безпеку дозволяють співробітникам усвідомлювати безпеку інформаційних систем і що вони повинні відповідним чином реагувати, коли виникають загрози. В організаціях, де недостатньо обізнаних у питаннях безпеки, співробітники не помічають очевидних ризиків безпеки, таких як віруси або крадіжка інтелектуальної власності, у своїх щоденних бізнес-справах. Незважаючи на запроваджені профілактичні заходи, як-от захист від зловмисного програмного забезпечення та брандмауер, ці заходи можуть лише частково вирішити наявну проблему, оскільки наївні та необізнані працівники можуть наражати організацію на дорогі помилки. Таким чином, наслідки недостатньої

поінформованості про безпеку становлять загрозу, так що навчання з питань безпеки стало критичним інструментом для зменшення кіберзагроз.

Незахищені мережі

Співробітники все частіше отримують доступ до внутрішніх мереж через власні пристрої, коли знаходяться поза робочим середовищем. Атаки можуть відбуватися у формі мережевого спуфінгу, акту маскування зв'язку з невідомого джерела як відомого, надійного джерела для отримання доступу до конфіденційних даних або запуску атак типу «Відмова в обслуговуванні» . Приклад того, як співробітники можуть стати жертвами атак спуфінгу, продемонструвала Investopedia (2020), яка фальсифікувала мережі в кафе у Великій Британії та просила потенційних користувачів надати PIN-код, який надсилався на їхні мобільні телефони для автентифікації. Результати показали, що третина випробуваних, які користувалися мережею в кафе, надали номери своїх мобільних телефонів, не усвідомлюючи, що це була атака [24].

1.3. Створення системи безпеки BYOD

Безпека BYOD має важливе значення для захисту корпоративних мереж. Захистити BYOD також складно через їх унікальність. Існує кілька рішень, спрямованих на вирішення проблем безпеки BYOD.

Рішення безпеки BYOD має відповідати наведеним нижче вимогам:

- Ізоляція простору: можливість ізолювати особистий простір і корпоративний простір на BYOD, щоб можна було застосовувати різні політики безпеки.
- Захист корпоративних даних: корпоративні дані мають бути зашифровані, коли вони зберігаються на BYOD; несанкціоновані або незаконні запити на доступ до корпоративних даних слід відстежувати та відхиляти.
- Застосування політики безпеки: можливість застосовувати політику безпеки підприємства щодо BYOD і гарантувати, що BYOD відповідають політикам безпеки підприємства.

Ці вимоги забезпечують бажаний контроль доступу, конфіденційність і керування політикою безпеки на BYOD. Ідеальне рішення BYOD має відповідати всім цим трьом вимогам безпеки. На рис 1.1. показано структуру безпеки BYOD у корпоративній мережі, яка відповідає всім цим вимогам. Структура включає дві сторони: корпоративну та BYOD [6].

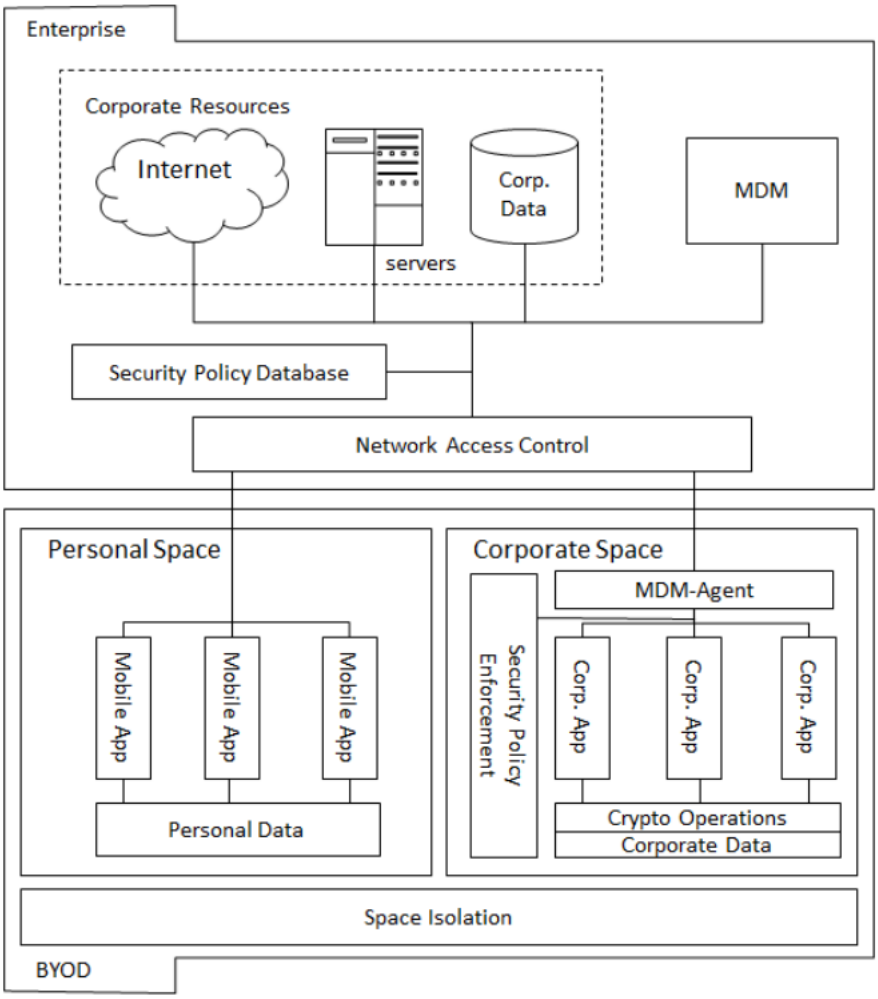


Рис.1.1. Схема системи безпеки BYOD

Корпоративна сторона включає різні корпоративні ресурси, такі як Інтернет, сервери та корпоративні дані, і забезпечує контроль доступу для BYOD для доступу до цих ресурсів. Запити на доступ надаються або відхиляються відповідно до політики безпеки підприємства. Підприємство також включає систему керування пристроями, наприклад MDM, для керування BYOD.

Контроль доступу до мережі надає точки доступу для BYOD і надає запити доступу BYOD відповідно до корпоративної політики безпеки. Контроль доступу до мережі повинен відрізняти запити від особистого та корпоративного простору

на BYOD. Використання різних сертифікатів для особистого та корпоративного простору є одним із варіантів диференціації цих послуг.

База даних політики безпеки визначає політики підприємства щодо обробки BYOD. Наприклад, як обробляти запити на доступ, що надходять із особистого простору на BYOD, який тип BYOD має доступ до мережі, який шифр використовуватиметься, який розмір ключа тощо.

MDM надає можливість керування BYOD. Він має функції збору управлінської інформації з BYOD і застосування певних політик безпеки на BYOD.

Сторона BYOD надає функції для ізоляції корпоративного простору, застосування політик безпеки та захисту корпоративних даних. Ізоляція простору надає можливість відокремити особистий простір від корпоративного простору на BYOD. Ізоляція простору необхідна для BYOD, щоб можна було застосовувати різні політики безпеки. Особистий простір включає в себе мобільні програми та особисті дані співробітників, які вони самостійно встановлюють.

Корпоративний простір включає корпоративні мобільні програми та корпоративні дані. Мобільні програми та дані в корпоративному просторі мають відповідати корпоративній політиці безпеки. В ідеалі особистий простір не повинен мати доступу до корпоративних ресурсів, але може мати обмежений доступ до певних ресурсів, таких як Інтернет. Можливо, є деякі програми, такі як SKYPE, які потрібні як для особистого, так і для ділового використання. Замість спільного використання програми між особистим простором і корпоративним простором, програми слід установлювати окремо в обох, щоб забезпечити безпеку корпоративних даних.

МДМ-Агент – це мобільний додаток, який встановлюється в корпоративному просторі. MDM-Agent надсилає інформацію про керування BYOD до MDM і діє як делегат від імені системних адміністраторів для застосування певних політик безпеки на пристрої. Наприклад, MDM може видати віддалену команду wipe і стерти всі корпоративні дані на BYOD [8].

Застосування політики безпеки гарантує, що BYOD відповідає політикам безпеки підприємства. Політики безпеки можуть включати, які криптографічні

операції слід використовувати, розмір ключів тощо. База даних політики безпеки (SPD) підтримується в корпоративному просторі. SPD містить таку інформацію, як тип даних, протоколи безпеки та ключі [9].

1.4. Методи управління мобільними користувачами концепції BYOD

Чітка та добре написана політика BYOD може бути першим кроком у забезпеченні контролю над безпекою та конфіденційністю середовища BYOD. Користувачі BYOD повинні дотримуватися деяких загальних вказівок щодо доступу та використання інформаційних ресурсів організації. Мета полягає не в обмеженні свободи користувача на його власних пристроях, а в тому, щоб запропонувати безпечне рішення, увімкнути дистанційну роботу та знайти рішення, яке буде виграшним для обох сторін. Ключові слова – добре організоване планування, зручність для користувача та пристрою, мінімальні обмеження та вимоги, конфіденційна інформація залишається приватною, відповідає вимогам ISO [13].

Таблиця 1.1

Етапи розробки політики BYOD

Етапи політики	Опис
Пристрої	1. Список пристроїв 2. ОС і версія пристрою Права адміністратора або root, зламано чи ні
Фізичний захист і доступ	4. Якщо можлива, багатофакторна аутенфікіція 5. Мінімум 6-значний пароль 6. Пароль для програм, де знаходяться інформація про компанії або інформація, що стосується компанії. Необхідна періодична зміна
Обмеження встановлення	7. Дозволити завантаження програмного забезпечення, яке зареєстроване в списку відомих 8. Інші завантаження не обмежені *

Етапи політики	Опис
програмного забезпечення	
Обмеження підключення до інформаційних сервісів	9. Дозволити всередині мережі лише відомі BYOD-s за списком відомих пристроїв 10. Дозволити можливість VPN 11. Не обмежувати підключення до публічного WIFI* 12. Навчити персонал розуміти безпеку, ризик публічних мереж і як захистити себе
Дистанційне вимкнення, стирання або блокування	13.Якщо пароль для додатків введено 5 разів неправильно, тоді блокування 14. Якщо пристрій загублено або вкрадено, тоді блокування
Криптографічні методи	15. Якщо пристрій потрапить до третіх рук або його вкрадуть, то криптографічні засоби повинні забезпечити безпеку інформації – надійний пароль, неможливість зробити копію, прочитати інформацію із зовнішнього пристрою
Захист від шкідливих програм	16. Захист від вірусів обов'язковий
Резервні копії	17. Резервне копіювання з BYOD заборонено* 18. Користувачам заборонено зберігати копії чи резервні копії інформації поза програмами, дозволеними організацією, або на інших приватних пристроях, які не входять до списка відомих пристроїв
Використання веб-сервісів і веб-додатків	18) Веб-програми та служби у внутрішній локальній мережі доступні лише за наявності з’єднання VPN

* Організація приймає на себе ризики та наслідки для зручності користувача

Добре почати розробку політики, але забезпечити дотримання політики може бути складно, якщо тільки працівник відповідає за свій пристрій. Програмне забезпечення «Mobile Device Management» дозволяють компаніям запроваджувати та керувати політикою, що робить MDM корисною не лише для політик BYOD. MDM означає будь-яку програму або інструмент, призначений для розповсюдження програм, даних і параметрів конфігурації на пристрої мобільного зв'язку. Дослідження стратегічної безпеки показує лише 33% з 1084 респондентів використовують програмне забезпечення для керування мобільними пристроями (MDM) для забезпечення єдиної політики безпеки. При виборі політики BYOD і систем MDM одним із найважливіших питань є те, які операційні системи підтримуватиме компанія [9].

Рішення MDM дозволяють підприємствам допомагати співробітникам ефективно виконувати свою роботу за допомогою мобільних пристроїв і водночас дозволяють підприємствам ефективно керувати всіма такими пристроями в організації. Кілька переваг MDM:

- Прості автоматичні оновлення програмного забезпечення на мобільних пристроях.
- Адміністратор може дистанційно контролювати та керувати пристроями.
- MDM пропонує можливість резервного копіювання та відновлення корпоративних даних.
- Можливість дистанційного відключення та блокування пристрою для запобігання несанкціонованому доступу в разі втрати чи пограбування пристроїв.

Системи MDM дистанційно відстежують стан мобільного пристрою для регулювання завдань.

Рис.1.2. ілюструє загальну схему корпоративної архітектури MDM. Таке рішення складається з двох основних елементів: сервера та агента, який є мобільним додатком. Агент MDM встановлюється на мобільний пристрій для постійної передачі інформації та статусу між мобільним пристроєм і сервером. Сервер підтримує запис отриманої інформації, а також передає на мобільний пристрій різноманітні команди/політики керування пристроєм, такі як стирання,

блокування, шифрування тощо. Системи керування мобільними пристроями також містять консоль MDM для адміністративного керування сервером MDM [2].

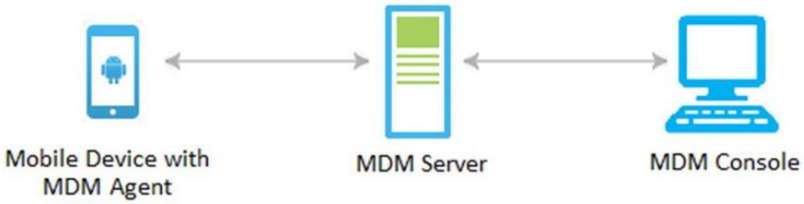


Рис.1.2. Схема архітектури Enterprise MDM

У такій архітектурі агент MDM встановлюється через playstore, де основною метою агента є надсилання інформації про користувача та даних мобільного пристрою на сервер MDM, а також застосування адміністративних команд, як-от дистанційне стирання та блокування, а також застосування відповідних політик.

Основні особливості MDM:

- Керування профілями: системи MDM налаштовують параметри політики та застосовують обмеження політики, щоб змінити функціонування пристрою відповідно до вимог компанії

- Відстеження місцезнаходження: дані відстеження можна використовувати для визначення поточного місцезнаходження пристрою та встановлення профілю руху пристрою.

- Віддалене блокування та стирання: мобільні пристрої можуть мати конфіденційні корпоративні дані та використовувати їх для доступу до кількох корпоративних служб. Консоль адміністратора може дистанційно заблокувати та стерти пристрій, щоб відновити його заводські налаштування, щоб уникнути витоку інформації, спричиненого збоєм або крадіжкою пристрою.

- Виявлення зловмисного програмного забезпечення: системи MDM можуть виявляти зловмисне програмне забезпечення в реальному часі, а потім вживати відповідних заходів і негайно створювати звіти.

- Резервне копіювання та шифрування даних: MDM може зберігати конфіденційну інформацію в зашифрованому просторі. Він також підтримує відновлення та резервне копіювання інформації.

- Чорний список URL-адрес: URL-адреси вносять до чорного списку відповідні URL-адреси веб-сайтів, що робить їх недоступними з браузера. Це може допомогти уникнути того, щоб співробітники витрачали час на певні веб-сайти, які не пов’язані з роботою. Додавання URL-адреси до чорного списку також є ефективним способом зупинити доступ до ймовірно шкідливих веб-сайтів.

Рішення MDM на підприємстві може забезпечувати лише певний рівень безпеки, якщо перед його розгортанням не було проведено ретельну перевірку вимог безпеки, пов’язаних із BYOD. Хоча цей процес зазвичай здійснюється на основі неофіційного аналізу вимог; точний формальний процес є важливим для забезпечення того, щоб ці вимоги безпеки були встановлені повністю та точно. Таким чином, на основі ризиків безпеки, пов’язаних із використанням мобільних пристроїв на підприємстві необхідно провести аналіз, щоб визначити відповідні вимоги безпеки для рішення MDM [7].

У міру того як технологічна індустрія продовжувала розвиватися, MDM ставав дедалі неспроможним задовольняти вимоги великих компаній. MDM починався як система для керувати пристроями та захисту IT-інфраструктури. Однак тепер компаніям потрібна можливість керувати цими пристроями на глибшому рівні.

Використання кількох інструментів керування кінцевими точками для керування та захисту різних кінцевих пристроїв у різних місцях призводить до великої кількості ручної та повторюваної роботи для відділів безпеки та IT-команд, а також підвищує ймовірність неузгодженості, неправильної конфігурації та помилок, які можуть зробити кінцеві точки та мережу вразливими до атак. . Unified Endpoint Management значно зменшує роботу та ризик завдяки створенню єдиної центральної інформаційної панелі, де IT-адміністратори та групи безпеки можуть переглядати, керувати та захищати кожен кінцевий пристрій, підключений до корпоративної мережі. Інструменти UEM працюють у всіх ПК і мобільних

операційних системах, включаючи Apple iOS і MacOS, Google ChromeOS і Android, Linux і Microsoft Windows. Багато рішень UEM також підтримують принтери та інші пристрої Інтернету речей для кінцевих користувачів, розумні годинники та інші носії, гарнітури віртуальної реальності, віртуальних помічників — усе, що працівник або бізнес-партнер може використовувати для підключення до мережі та виконання роботи [8].

UEM знає про всі пристрої в мережі незалежно від типу підключення, частоти підключення та місця підключення. Він навіть може виявляти підключені пристрої, про які не знають адміністратори або служби безпеки, у режимі реального часу. Інтеграція інструментів керування, систем корпоративного програмного забезпечення та сторонніх платформ в одне програмне забезпечення забезпечує кращий контроль і керування кінцевими точками. Системи UEM надають можливості керування пристроєм на одній панелі, спрощуючи керування кінцевими точками та операції безпеки. Перший крок до забезпечення комплексної безпеки передбачає отримання видимості всієї мережі підприємства. UEM забезпечує видимість на всіх кінцевих пристроях і підключених мережах, дозволяючи підприємствам відстежувати використання даних, системи вразливості тощо. Централізований підхід до безпеки та єдиний протокол безпеки дозволяють IT-командам керувати безпекою та відстежувати підозрілі дії на всіх пристроях. Це допомагає застосовувати політики безпеки на різних рівнях, щоб забезпечити суворий захист від усіх загроз. Крім того, IT-адміністратори можуть надавати персоналізований доступ до корпоративних даних і конкретних програм відповідно до місця розташування, моделей використання та бізнес-ролей. Основна мета розгортання рішення безпеки полягає в покращенні взаємодії з користувачем і продуктивності без шкоди для безпеки, і одне з цих рішень виконує саме це. Це позбавляє від необхідності керувати кінцевими точками за допомогою кількох інструментів, створюючи узгоджену взаємодію з користувачем і підвищуючи продуктивність [11].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ МОБІЛЬНИМИ КОРИСТУВАЧАМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ UNIFIED ENDPOINT MANAGEMENT

2.1. Призначення, можливості та функції Unified Endpoint Management

Щоб зрозуміти, як працює UEM, спочатку потрібно визначити, що собою являють EMM і CMT.

Управління мобільністю підприємства, або EMM, є еволюцією MDM, яка використовує контейнери для захисту програм і даних на мобільному пристрої. Незважаючи на те, що це забезпечує гнучкість BYOD, це все ще не вирішує проблему необхідності використання кількох інструментів керування на внутрішніх і зовнішніх пристроях.

Інструменти керування клієнтами, або CMT, допомагають IT-організаціям і організаціям підтримки автоматизувати адміністративні завдання кінцевих точок, такі як розгортання ОС, розповсюдження програмного забезпечення та керування виправленнями. Це передбачає налаштування та керування цими завданнями в мережі клієнтського пристрою [12].

UEM поєднують набори функцій MDM і CMT для забезпечення повного контролю та видимості кінцевих точок, підключених до мереж. Це робить UEM набагато ефективнішим методом керування кінцевими точками, ніж застарілі системи, особливо серед компаній із різноманітними пристроями. Це також забезпечує уніфіковане цифрове середовище на всіх пристроях і місцях.

Рішення UEM поєднують низку функцій, включаючи звітування, розширену автентифікацію користувачів, керування доступом і ізоляцію додатків, щоб підвищити безпеку та ефективність різноманітних мереж пристроїв. Рішення UEM забезпечують централізоване уявлення про всі кінцеві точки, підключені до мережі, а також дозволяють централізовано та віддалено керувати всіма цими кінцевими точками без необхідності компілювати дані з локальних і зовнішніх інструментів керування пристроями; рішення UEM охоплює їх усіх [18].

UEM також спрощує моніторинг використання та працездатності пристрою, включаючи вразливості, які потребують виправлення, оновлення ОС і оновлення програмного забезпечення чи програм, які потрібно розгорнути. У поєднанні ці функції дозволяють забезпечити базовий рівень безпеки та моніторингу загроз на кінцевих точках. Деякі рішення UEM навіть включають різноманітні вбудовані функції безпеки, які дозволяють захистити кінцеві точки від шкідливих програм, вірусів та шпигунського ПЗ.

Основна мета Unified Endpoint Management полягає саме в тому, що випливає з назви: дозволити керувати та контролювати всі кінцеві точки з одного центрального місця. Це означає, що рішення має підтримувати більшість різних типів кінцевих точок, які можуть підключатися до мережі, наприклад операційні системи Windows, Mac і Linux для настільних комп'ютерів і ноутбуків, iOS і Android для смартфонів і планшетів, а також пристрої IoT, такі як принтери та переносні пристрої.

Сама консоль керування запропонує цілий набір функцій, які можуть включати:

конфігурація розповсюдження програмного забезпечення та оновлення політики, конфігурація доступу на основі ролей, огляд користувачів, пристроїв і програм, підключених до мережі, справність пристрою/системні звіти про сповіщення, віддалене розповсюдження додатків і вмісту за допомогою автоматизованих розгортань для цільових груп користувачів, реєстрація нового користувача та пристрою [14].

Через зростаючу складність атак соціальної інженерії та технології злому паролів потрібно переконатися, що перевіряється кожен користувач, коли він намагається підключитися до корпоративних даних через свою кінцеву точку. Найпростіший спосіб зробити це за допомогою багатофакторної автентифікації (MFA). MFA — це метод підтвердження особи, який вимагає від користувачів підтвердити свою особу двома чи більше способами, перш ніж їм буде надано доступ до програми, системи чи мережі. Вони можуть це зробити трьома основними способами: використовуючи те, що вони знають, наприклад PIN-код,

те, що вони мають, наприклад програму автентифікації, щось, що стосується біометричних даних користувача, наприклад сканування відбитків пальців. MFA гарантує, що зловмисники не зможуть отримати доступ до облікових записів співробітників, навіть якщо їм вдасться отримати пароль. Рішення UEM має мати вбудований або інтегрований MFA. Крім того, він повинен включати систему єдиного входу (SSO), що означає, що користувачі повинні пройти автентифікацію лише після того, як пристрій перебував у режимі офлайн протягом встановленого періоду, а не щоразу, коли вони намагаються відкрити нову програму. Це допоможе зберегти корпоративні дані в безпеці в разі втрати або викрадення пристрою, гарантуючи, що цей захист не перешкоджатиме продуктивності співробітників.

Ізоляція додатків є особливо важливою функцією, впроваджуєте рішення UEM на пристроях BYOD. Ця функція дозволяє співробітникам розділяти свої особисті та робочі програми та безпечно використовувати їх на одному пристрої. Пропонований рівень ізоляції відрізняється в різних рішеннях. Деякі з них дозволяють користувачам створити окреме «робоче середовище» на своєму пристрої, де безпечно зберігаються робочі програми та дані. Деякі дозволяють користувачам підключатися до корпоративної внутрішньої мережі зі свого пристрою. Інші пропонують режими «контейнера» або «кіоску», які надають адміністраторам вищий рівень контролю (наприклад, можливість керувати налаштуваннями периферійних пристроїв або переглядати екран пристрою в режимі реального часу) над пристроями своїх користувачів, коли вони активовані, для ситуацій, коли потрібен підвищений рівень безпеки [13].

Усі рішення UEM мають надавати інформацію про використання пристрою та вразливості, щоб допомогти налаштувати політики та впровадити всі необхідні заходи безпеки для захисту пристроїв мережі. Найкращі рішення також дозволять реалізувати цей захист за допомогою потужних інтеграцій; деякі мають ці вбудовані функції безпеки. Вони можуть включати:

- VPN, щоб гарантувати, що мережеві з’єднання завжди безпечні, навіть коли співробітники підключаються через незахищені мережі Wi-Fi, такі як персональні домашні маршрутизатори або безкоштовні хмарні служби;

- Віддалене стирання або блокування пристрою в разі втрати або викрадення пристрою;
- Автоматичне блокування пристрою після певного періоду бездіяльності для захисту від втрати або крадіжки інформаціїї;
- Безпека електронної пошти, яка гарантує, що на підключеному пристрої можна відкрити лише надійні корпоративні вкладення;
- Регулювання налаштувань дистанційного периферійного пристрою, наприклад гучності або яскравості екрана, і дистанційний перегляд екрана [15].

2.2. Призначення, можливості та функції Unified Endpoint Management від ManageEngine

Unified Endpoint Management від ManageEngine — це веб-додаток для адміністрування та керування робочим столом. Ця програма дозволяє адміністраторам ефективно керувати комп'ютерами з центральної точки. Він містить такі функції, як розгортання програмного забезпечення, керування виправленнями, встановлення пакета оновлень, керування ресурсами, розгортання ОС, віддалене керування, конфігурації, системні інструменти, звіти Active Directory і звіти про вхід користувача. ManageEngine Endpoint Central вимагає завантаження та встановлення агента на всіх пристроях, якими керуватиме Endpoint Central. Адміністратори можуть увійти в онлайн-портал, щоб керувати пристроями та призначеними для них користувачами [10].

Керування виправленнями **(**Patch Management**)** дозволяє адміністраторам відстежувати стан виправлень на кожному керованому пристрої. Це дозволяє Endpoint Central бачити, чи на деяких пристроях відсутні будь-які виправлення, і чи є ці виправлення критичними чи ні. У розділі «Керування виправленнями» є інформаційна панель, яка надає графіки стану системи, справності мережі, відомості про те, яких виправлень бракує, а також керовані комп'ютери за їхніми операційними системами. У ньому також є розділ, присвячений показу останніх новин безпеки. Адміністратор може вибрати всі виправлення, які він хоче

встановити, натиснути «Установити», а потім створити конфігурацію. Під час процесу створення конфігурації адміністратори можуть планувати розгортання виправлень на основі вибраної політики розгортання. Тут адміністратор також вибирає, на яких пристроях він хоче розгорнути виправлення. Патчі також можна автоматизувати. Адміністратори можуть створити автоматичне завдання для встановлення патчів, оновлень сторонніх розробників, оновлень антивірусної програми та драйверів. Ці автоматичні виправлення можна відкласти, якщо необхідно, вказавши кількість днів очікування або від випуску виправлення, або від дати затвердження.

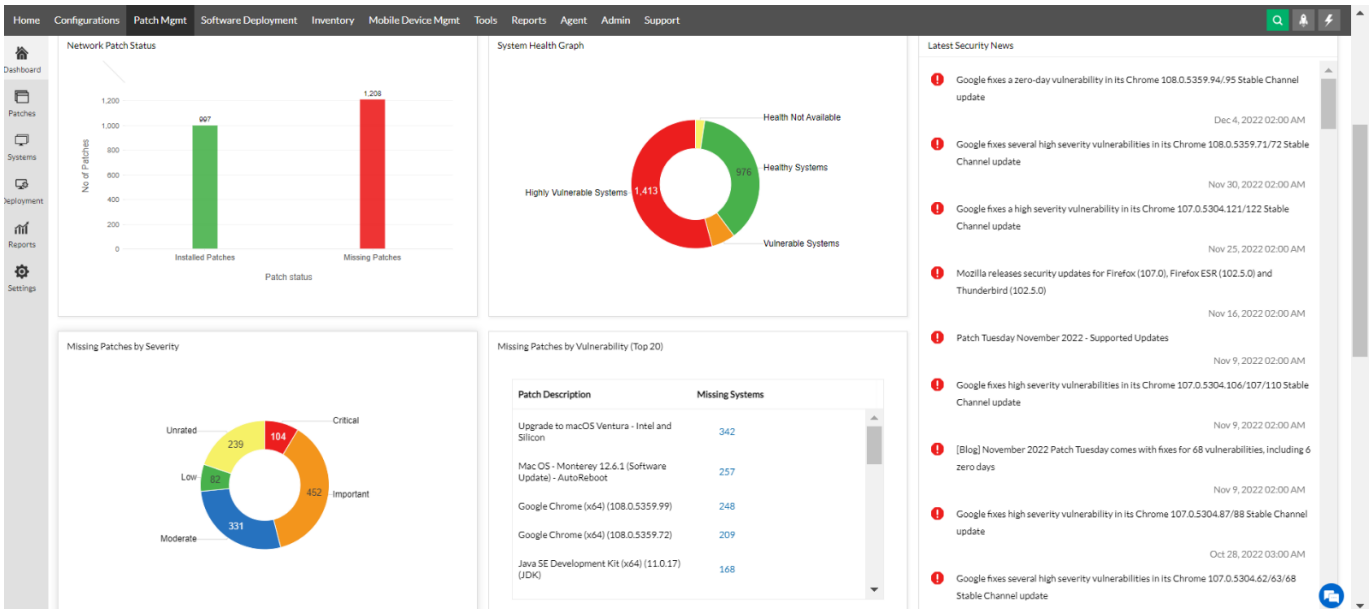


Рис.2.1. Інтерфейс вкладки «Patch Management»

Керування програмним забезпеченням контролює, яке програмне забезпечення можна, а яке не можна інсталювати на керованих пристроях. Він також може створити список усіх програм, встановлених на пристрої. Адміністратор може автоматизувати розгортання програмного забезпечення за допомогою шаблонів, попередньо налаштованих у Desktop Central. Ці шаблони програмного забезпечення сприяють швидкому створенню та розгортанню пакетів програмного забезпечення, надаючи всю необхідну інформацію про програмне забезпечення для адміністратора. Після того, як все необхідне програмне забезпечення буде додано до пакетів, адміністратор може запустити процес

встановлення, створивши нову конфігурацію. Пакети також можна видалити, дотримуючись того самого процесу, описаного вище, і замінивши встановлення на видалення. Рис. 2.2 ілюструє процес розгортання програмного забезпечення.

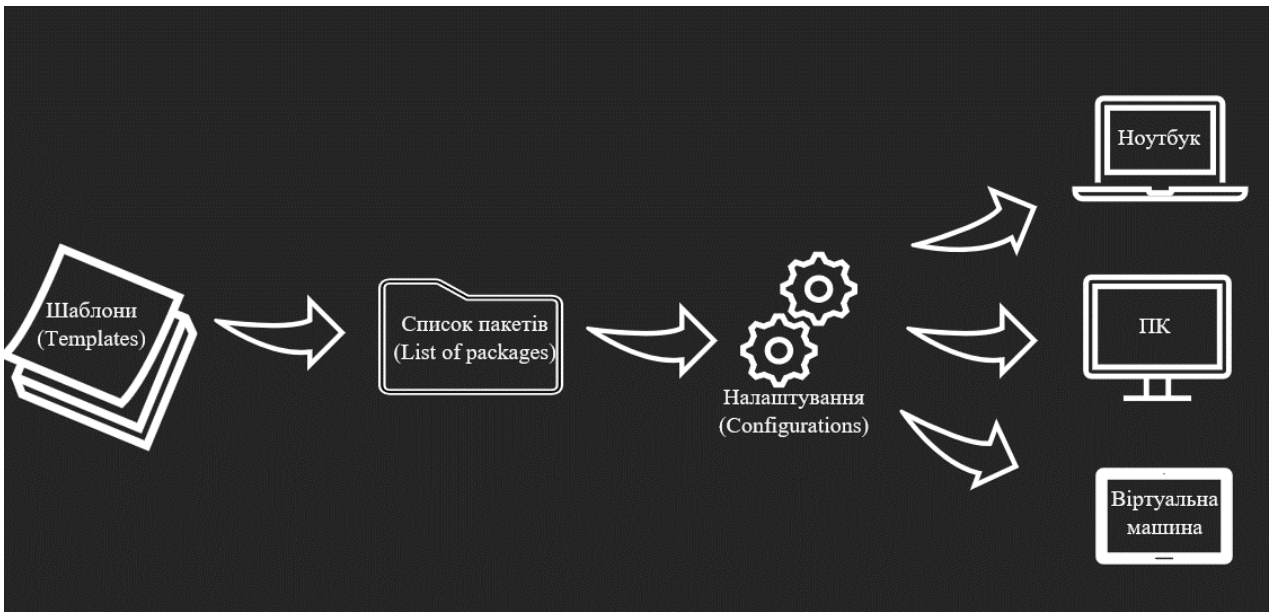


Рис.2.2. Процес розгортання програмного забезпечення Endpoint Central

Вкладка «Inventory» містить багато різних розділів, які охоплюють комп’ютери, обладнання, програмне забезпечення, сповіщення та звіти. В розділі комп’ютери можна переглядати поточні керовані комп’ютери, додавати нові комп’ютери та змінювати дані про них.

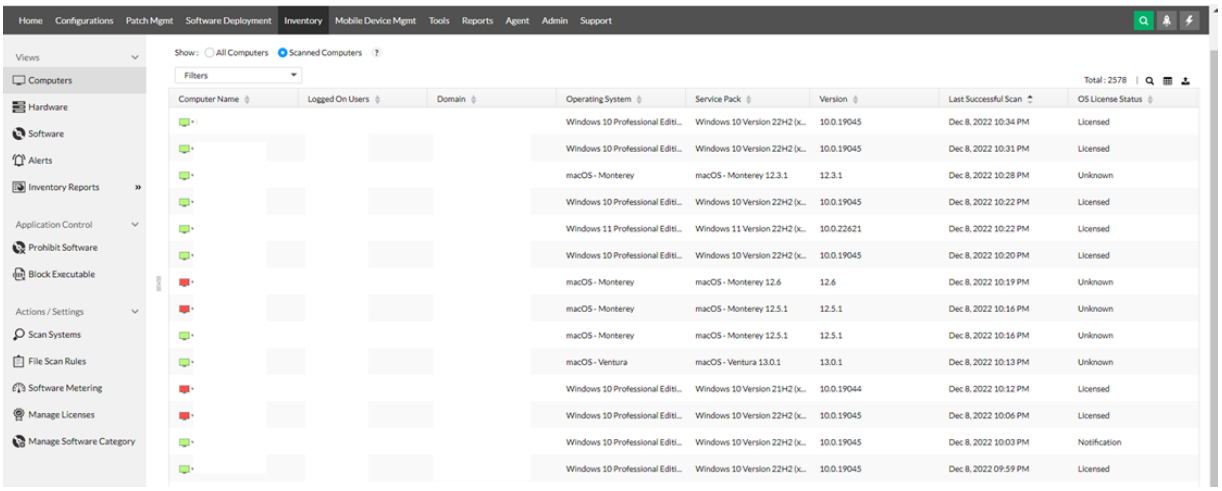


Рис.2.3. Інтерфейс вкладки «Inventory»

Якщо перейти на один із комп’ютерів у списку, відкриється вікно з детальною інформацією про вибраний комп’ютер. Детальна інформація розбита на

багато різних вкладок. Ці вкладки: Зведення, Система, Обладнання та Програмне забезпечення. Вкладка «Summary» містить детальний огляд комп'ютера. На вкладці «System» перераховані всі служби, користувачі, групи та драйвери, які є на комп'ютері. На вкладці «Hardware» наведено всі відомості про апаратне забезпечення вибраного комп'ютера. На вкладці «Software» перелічено все програмне забезпечення, встановлене на пристрої.

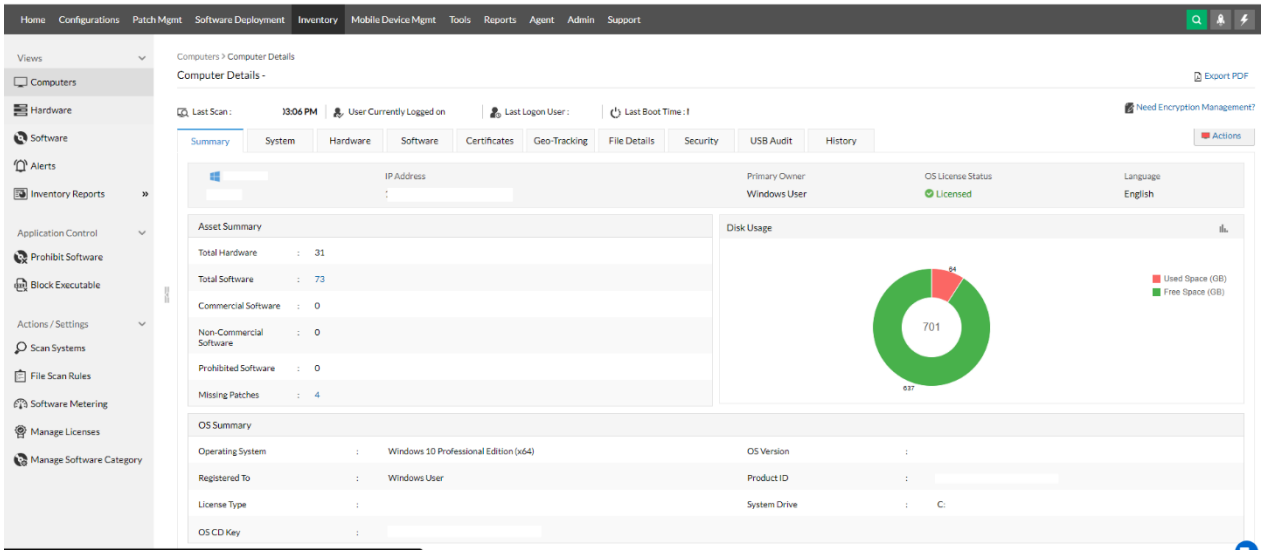


Рис.2.3. Інтерфейс вкладки «Computer Details»

Керування мобільними пристроями дозволяє адміністраторам реєструвати комп'ютери та мобільні пристрої та керувати ними. Розділ «Mobile Device Management» також керує будь-якими програмами для мобільних пристроїв, які організація вирішила використовувати. Адміністратори можуть налаштувати керований доступ облікових записів, або самостійно додавати їх вручну за допомогою вбудованої функції пошуку програм Endpoint Central. Потім ці програми можна призначити будь-якому мобільному пристрою, яким керує EndpointCentral. Таким же чином можна керувати програмами для Windows і Mac.

Керування живленням є частиною ManageEngine Endpoint Central, яка дозволяє визначати та застосовувати схеми живлення для пристроїв Windows, Mac і Linux. Ці схеми живлення визначають, коли пристрої вимкнуть дисплей, перейдуть у режим сну, сплячий режим і вимкнуть жорсткий диск. Наприклад, є

можливість налаштувати схему живлення, згідно з якою система переходитиме в режим сну після 1 хвилини бездіяльності комп’ютера [11].

Також можена використовувати керування живленням, щоб вимкнути всі комп’ютери в неробочий час або налаштувати політики для планування вимкнення для груп комп’ютерів. Наприклад, якщо працівники закінчують роботу о 17:00, можна налаштувати правила вимкнення їхніх пристроїв о 17:00, щоб вам не довелося робити це вручну.

Управління IT-активами — платформа надає можливості керування IT-активами, які дають змогу сканувати вашу мережу на наявність нещодавно доданих апаратних і програмних активів і отримувати сповіщення про зміни у середовищі за допомогою попереджень інвентаризації в реальному часі. Процес управління активами пропонує ряд варіантів конфігурації. Наприклад, є можливість визначити частоту запланованих сканувань і чи потрібно запускати сканування щоденно, щотижня чи щомісяця. Також можете проводити сканування за вимогою.

Так само можна налаштувати сповіщення, щоб система сповіщала щоразу про додавання чи видалення пристроїв введення/виведення, пристроїв зберігання даних, логічних пристроїв, пам’яті чи елементів керування. Це допомагає точно знати, які пристрої підключено до вашої мережі.

Платформа може автоматично створювати образи дисків робочого або вимкненого комп’ютера, а потім додавати їх до централізованого сховища. Потім, коли їх буде збережено, користувачі зможуть використовувати налаштовані шаблони розгортання для розгортання образів дисків на основі ролі кожного співробітника. Потім розгортається новий образ диска, користувач може реалізувати конфігурації після розгортання. Наприклад, під час розгортання оновлення на комп’ютері користувач може налаштувати систему на автоматичне встановлення нових програм або файлів EXE на пристрої. Функції, надані платформою, створюють міцну основу для автоматизації створення образів і розгортання ОС і позбавляють адміністраторів необхідності витрачати час на керування ними вручну.

ManageEngine Endpoint Central також пропонує кілька надбудов безпеки кінцевих точок, які можна використовувати для захисту пристроїв від зовнішніх загроз з точки зору безпеки. Наприклад, доповнення керування вразливістю дає змогу запускати сканування вразливостей на кінцевих точках, щоб виявляти неправильні конфігурації та вразливості, які піддають пристрої ризику зламу. Є функція проводити перевірки програмного забезпечення, щоб виявити небезпечне, шкідливе та неавторизоване програмне забезпечення на своїх пристроях. Це поширюється на антивірусні перевірки, які дозволяють побачити, чи поточний антивірус оновлений чи неактивний. Платформа також пропонує захист від загроз на рівні програми. За допомогою надбудови для керування програмами можна створювати білі списки, щоб визначати, які програми схвалені, і чорні списки, які блокують неприйнятні та шкідливі програми по всій мережі. Ці конфігурації дозволяють легко переконатися, що законні програми підтримуються, а шкідливі програми видаляються.

Функція гарантійного відстеження Endpoint Central (рис.2.4.) дозволяє записувати гарантійну інформацію пов’язаних IT-обладнання, що використовується на підприємстві. За допомогою цього програмного забезпечення для відстеження гарантії можна вводити такі деталі, як сервісний тег, дата покупки та закінчення терміну дії активу тощо. Агент Endpoint Central, який знаходиться на клієнтській машині, сканує різні деталі активу. Ця інформація надсилається на центральний сервер кінцевої точки та перевіряється за допомогою вхідних даних, які були записані раніше. Абсолютно не потребуючи втручання IT-адміністратора організації, є можливість автоматизувати весь процес керування гарантіями за допомогою програмного забезпечення для відстеження гарантій.

Для системних адміністраторів дуже важливо використовувати програмне забезпечення для керування гарантіями на обладнання та програмне забезпечення у своїй організації, щоб відстежувати гарантійні деталі IT-активів, якими вони керують, і використовувати додатковий захист для продуктів у разі пошкодження чи несправності. Будь то тріщина на екрані, помилка в оперативній пам’яті, збій жорсткого диска чи будь-яка передчасна несправність комп’ютера, програмне

забезпечення для відстеження гарантії гарантує, що ви не втратите гарантію, якою ви могли скористатися, щоб замінити чи виправити його . Система управління гарантіями збільшує шанси на підвищення якості програмного та апаратного забезпечення, що сприяє підвищенню продуктивності.

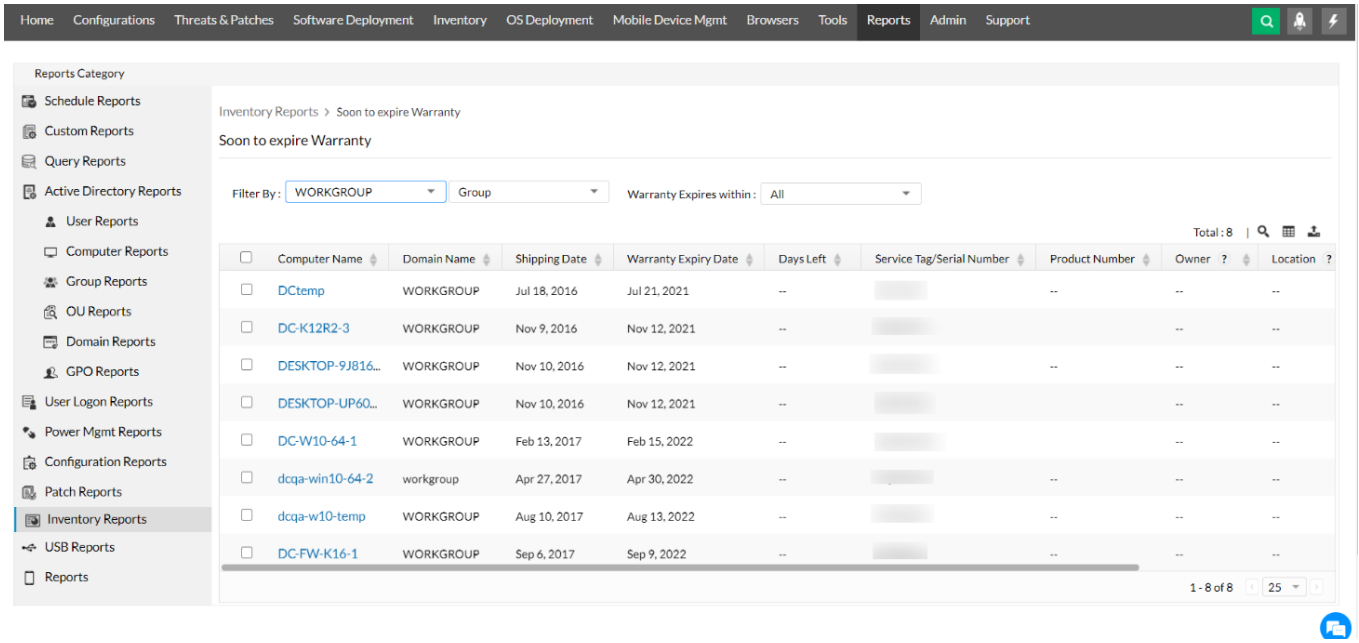


Рис.2.4. Функція гарантійного відстеження Endpoint Central

Інструмент віддаленого доступу значною мірою допомагає IT-адміністраторам і робить процес усунення несправностей швидшим і надійнішим. Endpoint Central надає доступ до безлічі функцій віддаленого доступу , як показано на рис 2.5.

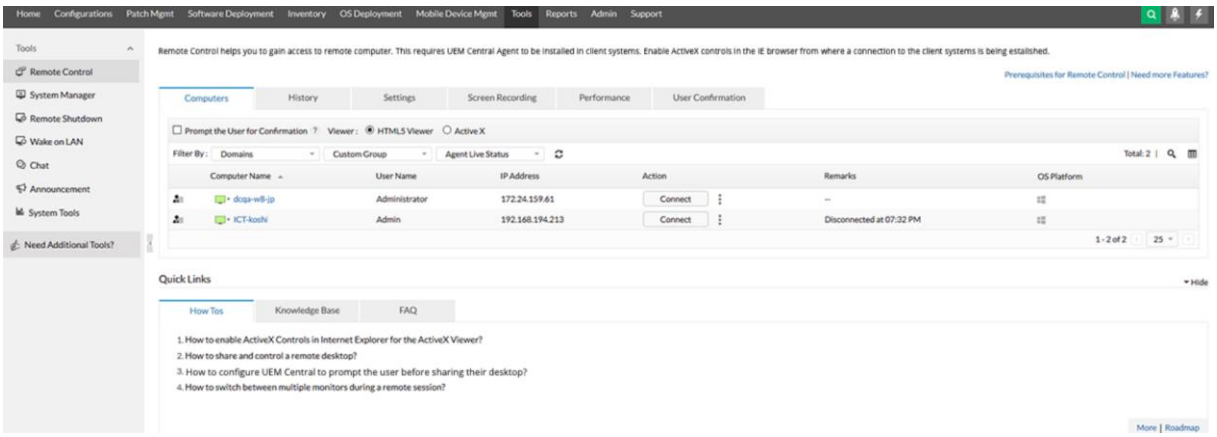


Рис.2.5. Інтерфейс вікна віддаленого доступу

1. Підтримка кількох моніторів: віддалена машина може мати більше одного активного монітора. Після встановлення віддаленого з’єднання відображатимуться всі активні монітори.

2. Передача файлів: файли можна динамічно передавати під час віддаленого сеансу, що робить його продуктивним. Залежні файли можна додати або видалити під час усунення несправностей.

3. Заблокувати монітор кінцевого користувача та вимкнути введення: Щоб вирішити проблеми швидше, може знадобитися повний контроль над комп’ютером без втручання користувача.

4. Запис віддалених сеансів: записані віддалені сеанси можна використовувати для освітніх цілей та аудиту. Якщо у організації є нові співробітники, записані сеанси можна передати їм для навчання.

5. Захист конфіденційності кінцевих користувачів: якщо дотримання вимог HIPAA або PCI є проблемою, рекомендується отримати дозвіл користувача перед встановленням віддаленого з’єднання. Цю опцію отримання дозволу можна зробити постійною за допомогою Endpoint Central.

6. Усунення несправностей із мобільного пристрою: ініціювання віддаленних сеансів та вирішення проблеми з комп’ютерами будь-де та будь-коли за допомогою мобільних пристроїв.

Використання портативних пристроїв зберігання даних створює дві основні проблеми для організації: крадіжка даних і ін’єкція зловмисного програмного забезпечення. За відсутності комплексного програмного забезпечення для керування USB-пристроями незадоволеному працівнику надзвичайно легко ввести зловмисне програмне забезпечення або викрасти важливу для бізнесу інформацію за допомогою USB-пристрою. Щоб запобігти подібним речам, IT-командам необхідно ввести суворі обмеження на USB пристрої за допомогою відповідного керування безпекою, щоб забезпечити контроль USB-пристроїв. Функції безпечного керування USB Endpoint Central допомагають адміністраторам обмежити використання USB-пристроїв вибірково на основі різних ролей і відділів.

Цей аспект керування USB-пристроями дозволяє адміністраторам централізовано контролювати використання різних USB-пристроїв у мережі, блокуючи або вимикаючи їх. Це запобігає несанкціонованому завантаженню, а також можливості запровадження шкідливого програмного забезпечення в мережу. Використовуючи програмне забезпечення для керування безпекою USB, обмеження можна встановити не лише на рівні комп'ютера та користувача, але й на типі виробника, забезпечуючи більшу доступність.

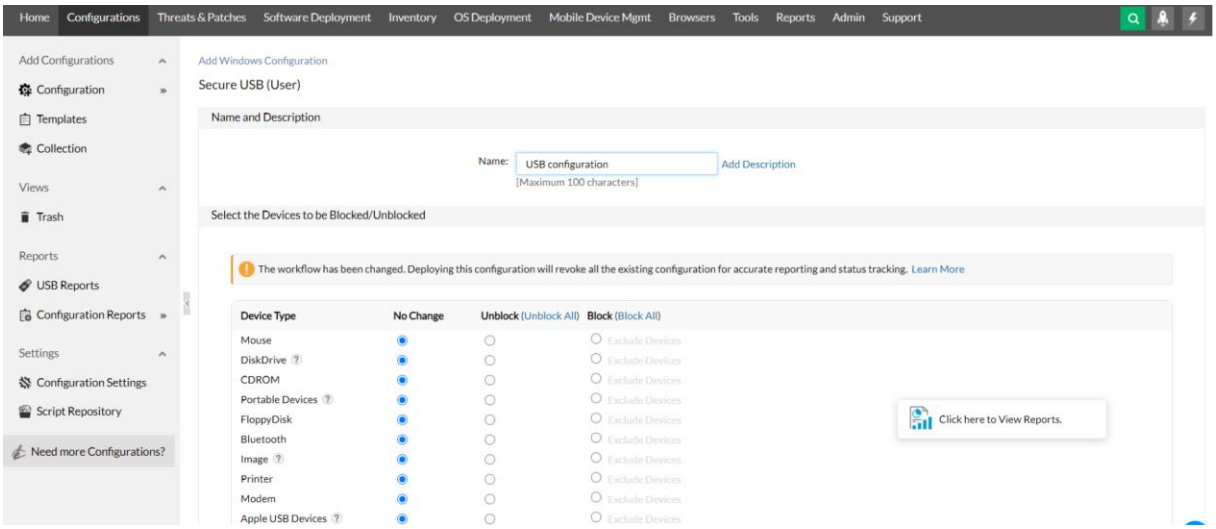


Рис.2.6. Керування безпекою пристрою USB

IT-команди стикаються з громіздким завданням аналізу використання ручних накопичувачів, компакт-дисків або будь-яких інших портативних пристроїв зберігання даних, які можуть загрожувати даним або безпеці компанії. Завжди краще записувати ці дії для майбутнього аудиту за допомогою диспетчера пристроїв USB. Програмне забезпечення для керування безпекою USB від Endpoint Central допомагає відстежувати використання зазначених USB-пристроїв і надає всю необхідну інформацію, наприклад:

- Ім'я пристрою
- Ім'я користувача
- Тип пристрою
- Тривалість часу
- Виробник та інше.

Після того, як USB-пристрій було обмежено, можна налаштувати параметри сповіщень USB, щоб повідомляти користувачів щоразу, коли вони підключають заборонений пристрій. Таким чином, IT-групи можуть використовувати функції керування USB-пристроями Endpoint Central і гарантувати, що кінцевий користувач дотримується політики обмеження USB, встановленої організацією.

Керування та контроль USB-пристроїв – це процес моніторингу та обмеження використання USB-пристроїв у мережі для захисту від внутрішніх загроз. Керування пристроєм USB є обов'язковим для безпеки кінцевих точок і даних, а належне програмне забезпечення для керування безпекою USB запобігає загрозам.

Endpoint Central поставляється з інтегрованим набором звітів, який демонструє повний і вичерпний список звітів. Від інформації, що стосується деталей входу користувача, до інвентаризації, пов'язаної з мережею, це допомагає IT-адміністраторам отримувати цілу низку інформації навіть із Active Directory свого підприємства всього за кілька клацань мишкою. Управління робочим столом можна спростити за допомогою параметрів планування програмного забезпечення. Ці звіти отримують інформацію та відображають її у добре відформатованому вигляді. Параметри перетворення вилученого звіту в інші формати файлів, як-от PDF і CSV.

Звіти про керування сервером і робочим столом, інтегровані з програмою, можна класифікувати як:

- Звіти про конфігурацію
- Звіти про управління живленням
- Звіти про виправлення
- Звіти про інвентарізацію
- Звіти про вхід користувача
- Звіти Active Directory

Звіти про конфігурацію пов'язані з певним користувачем або комп'ютером. Звіт про конфігурацію робочого столу на основі певного типу конфігурації також

можна отримати за допомогою програмного забезпечення. Ці звіти дуже корисні під час аудитів.

Оскільки ініціативи Go-Green поширюються в корпоративному світі, на адміністраторів покладається додатковий тягар щодо збереження енергії. Додаток може допомогти адміністраторам перейти в режим енергозбереження, використовуючи свої повноваження з керування живленням. Звіт про час роботи та простою системи може бути корисним для розробки стратегії енергозбереження на підприємстві.

Звіти про виправлення надають детальну інформацію про вразливі системи у вашій мережі разом із деталями виправлення для усунення цієї вразливості. Додаток періодично сканує системи та визначає вразливість після перевірки відсутності відповідних виправлень. Різноманітні звіти про виправлення, які пропонуються, включають:

- звіт про вразливі системи;
- звіт про вразливі виправлення;
- звіт про підтримувані виправлення;
- звіт про стан завдання.

Звіти про інвентарізацію надають повну інформацію про весь інвентар у мережі. Важливу інформацію, як-от відповідність ліцензії та відомості про вимірювання програмного забезпечення, можна легко отримати, створивши звіти про інвентаризацію. Доступні окремі звіти про інвентаризацію обладнання та програмного забезпечення. Доступні фільтри також можуть бути застосовані для вилучення цілого ряду корисної інформації, яка може знадобитися.

Звіти про вхід користувача надають набір інформації, пов’язаної з активністю входу користувача. Продукт пропонує спеціальні звіти, що стосуються подробиць входу/виходу, історії входу тощо. Комп’ютери, на яких жоден користувач ніколи не входив у систему, також можна знайти за допомогою готового звіту. Оскільки звіти базуються на агентах, вони є більш точними та містять такі відомості, як час входу та виходу користувача, комп’ютер, з якого він увійшов, контролер домену, про який він повідомив, тощо, а також історію входу.

Звіти Active Directory надають IT-адміністратору всі важливі відомості про інфраструктуру та об’єкти AD у налаштуваннях Windows. Endpoint Central спеціалізується на створенні звітів AD і пропонує можливість створення звітів без сценаріїв для IT-персоналу. Створені звіти Active Directory полегшують періодичні перевірки відповідно до стандартів відповідності.

Є можливість створити будь-яку кількість ролей у Endpoint Central і надати їм дозволи на свій вибір відповідно до особистих потреб. Потім ці ролі можна пов’язати з користувачами Endpoint Central. Також є набір попередньо визначених ролей, які стають у нагоді:

- Адміністратор. Роль адміністратора означає суперадміністратора, який здійснює повний контроль над усіма модулями.
- Гість. Роль гостя зберігає дозвіл лише на читання для всіх модулів.
- Технік. Роль техніка має чітко визначений набір дозволів для виконання певних операцій. Користувачам із роллю Технік заборонено виконувати всі операції, перелічені на вкладці Адміністратор.
- Аудитор. Роль Аудитора створена спеціально для цілей аудиту. Ця роль допоможе надавати аудиторам дозволи переглядати деталі інвентаризації програмного забезпечення, перевіряти відповідність ліцензії тощо.
- Роль засобу перегляду віддаленого робочого столу. Роль засобу перегляду віддаленого робочого стола дозволить користувачам, пов’язаним з нею, викликати підключення до віддаленого робочого столу та переглядати відомості про користувачів, які підключилися до певної системи.
- Менеджер IT-активів – менеджер IT-активів має повний доступ до модуля керування активами, а всі інші функції недоступні.
- Менеджер виправлень. Роль менеджера виправлень має повний доступ до модуля керування виправленнями, а всі інші модулі/функції недоступні.
- Диспетчер мобільних пристроїв – Диспетчер мобільних пристроїв має повний доступ до модуля MDM, а всі інші модулі/функції недоступні [21].

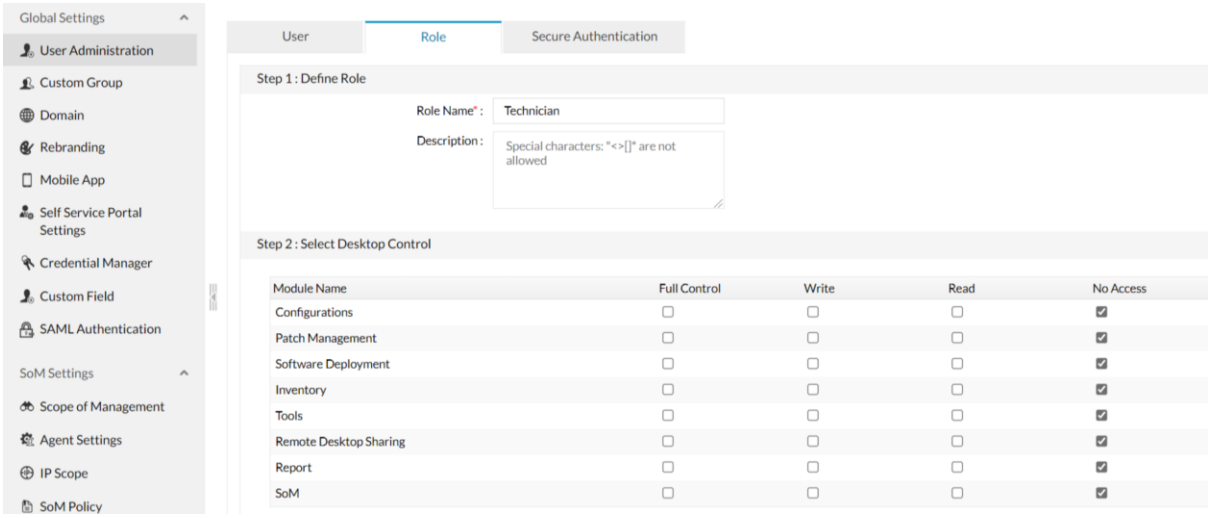


Рис.2.7. Контроль доступу на основі ролей

2.3. Компоненти та архітектура рішення Unified Endpoint Management від ManageEngine

Центральний сервер Endpoint розташований на сайті замовника. Сервер дає змогу виконувати різноманітні завдання керування робочим столом, щоб допомогти адміністраторам ефективно керувати комп’ютерами в мережі компанії. Деякі із завдань включають наступне:

- Встановлення агента на комп'ютери в мережі замовника.
- Розгортання конфігурацій.
- Сканування інвентарю та виправлень.
- Формування звітів. Наприклад, звіти, пов’язані з компонентами інфраструктури Active Directory.

Рекомендується взагалі не вимикати центральний сервер кінцевої точки. Його слід постійно вмикати, щоб щодня виконувати різноманітні завдання керування робочим столом. Усі завдання керування робочим столом можна виконувати за допомогою консолі продукту.

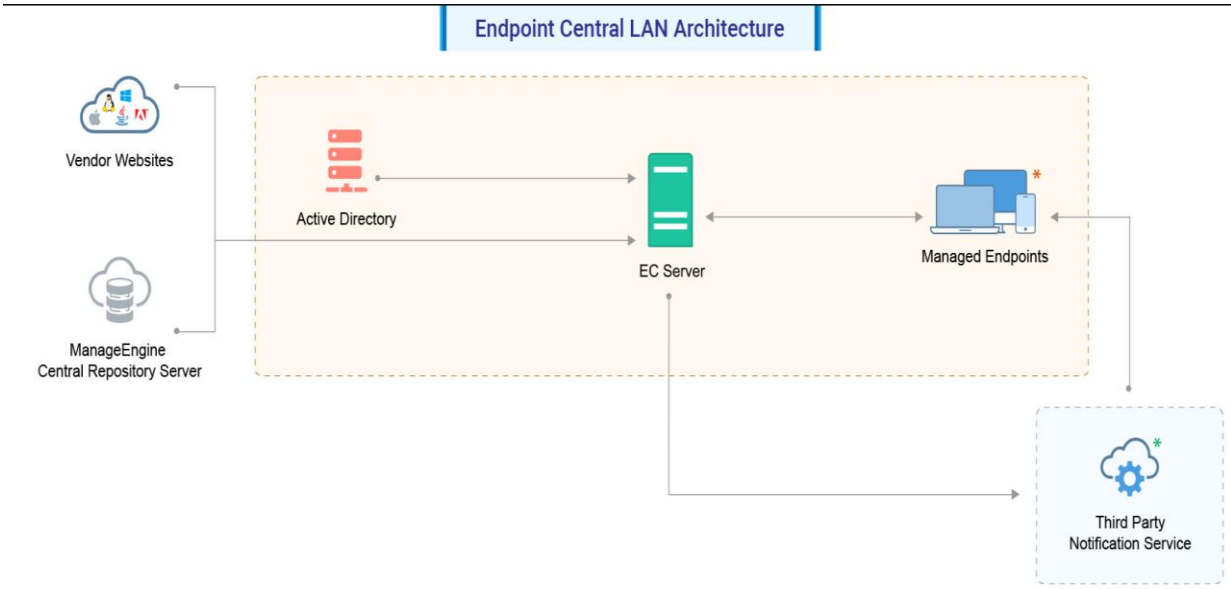


Рис.2.8. Архітектура локальної мережі Endpoint Central

Агент Endpoint Central — це програма, яка встановлюється на комп'ютерах, якими керують за допомогою Endpoint Central. Він автоматично встановлюється на комп'ютери в локальній мережі. Це допомагає виконувати різні завдання, ініційовані на сервері Endpoint Central. Наприклад, для того, щою видалити програмне забезпечення з комп'ютера у мережі, можна зробити необхідні налаштування для цього завдання на сервері Endpoint Central. Агент відтворює ці налаштування та забезпечує ефективне виконання завдання.

Агент також оновлює сервер Endpoint Central за допомогою статусу розгорнутих конфігурацій. Він періодично перевіряє сервер Endpoint Central на наявність інструкцій, пов'язаних із завданнями, і виконує їх. Агент зв'язується з сервером, коли відбуваються такі дії:

- Конфігурації для користувача: авторизація користувачів, 90-хвилинний інтервал оновлення.
- Спеціальні конфігурації комп'ютера: запуск комп'ютера, 90-хвилинний інтервал оновлення.

База даних виправлень — це портал на веб-сайті ManageEngine. Він містить найновішу базу даних уразливостей, яка публікується після тестування виправлень. Центральний сервер Endpoint періодично синхронізує цю інформацію та сканує

комп’ютери в мережі, щоб визначити, які патчі відсутні. Відсутні патчі встановлюються на комп’ютерах, на яких їх немає.

Зв’язок між сервером Endpoint Central і базою даних виправлень відбувається через проксі-сервер, або через пряме з’єднання з Інтернетом. Необхідні патчі завантажуються з веб-сайтів відповідних постачальників і зберігаються на сервері Endpoint Central перед розгортанням їх на комп’ютерах у мережі. Агенти копіюють необхідні двійкові файли виправлень із сервера Endpoint Central.

Веб-консоль продукту є центральною точкою, з якої адміністратор може керувати всіма завданнями, пов’язаними з керуванням робочим столом. Доступ до цієї консолі можна отримати з будь-якого місця. Наприклад, до нього можна отримати доступ через LAN, WAN і з дому через Інтернет або VPN. Для доступу до веб-консолі не потрібні окремі інсталяції клієнта.

У налаштуваннях домену на основі Active Directory сервер Endpoint Central збирає дані з Active Directory для створення звітів для наступного:

- сайти;
- домени;
- організаційні одиниці (OU);
- групи;
- відомості про комп'ютери;

Це дає адміністраторам доступ до всієї інформації, яка зберігається в Active Directory [10].

3 РОЗРОБЛЕННЯ ВАРІАНТА УПРАВЛІННЯ МОБІЛЬНИМИ КОРИСТУВАЧАМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ КОНЦЕПЦІЇ BYOD

3.1 Розроблення технологіїуправління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD

Хоча пристроями в середовищі BYOD потрібно керувати для захисту корпоративних даних, повний моніторинг і контроль пристроїв, що належать працівникам, може призвести до того, що працівники вважатимуть це порушенням їхньої конфіденційності та активно протистоять управлінню BYOD. Крім того, запрошення співробітників використовувати їхні особисті пристрої може призвести до широкого розмаїття типів пристроїв і платформ, залучених до робочого процесу. Може бути важко забезпечити стабільний рівень контролю над усіма цими пристроями. Щоб подолати ці проблеми, організації повинні розробити чітку політику BYOD і використовувати хороший інструмент управління BYOD [13].

Технологія розроблення політики BYOD:

- Організація та співробітники BYOD розподіляють відповідальність за інформаційну безпеку та конфіденційність.
- Пристрої зі зламаним доступом і рутовані пристрої заборонені до використовування як BYOD. Вони розглядаються як небезпечні, пристрої з порушенням конфіденційності, тому піддаються впливу загроз та вразливостей.
- Корпоративну інформацію можна отримувати, змінювати, обробляти, зберігати та передавати на пристроях BYOD лише за умови успішної реєстрації пристрою/підключення.
- Інформацію, яка класифікується як суворо конфіденційна, заборонено змінювати або зберігати на пристроях BYOD.
- Користувачі BYOD повинні використовувати лише методи автентифікації, такі як ідентифікатор користувача та пароль, схвалені IT-керівництвом організації.

- Усі пристрої BYOD повинні використовувати блокування екрана з паролем, який автоматично блокує пристрій у режимі очікування.
- Організація має право контролювати свою інформацію на пристроях BYOD, а також обмежувати або блокувати доступ пристроїв BYOD до корпоративних інформаційних ресурсів і активів.
- Користувачам BYOD рекомендується не завантажувати та не встановлювати будь-який шкідливий контент або програми на свої пристрої. У разі порушення безпеки або конфіденційності внаслідок завантаження шкідливого контенту/додатків повну відповідальність несе власник пристрою.
- Користувачі BYOD несуть відповідальність за резервне копіювання даних своїх пристроїв, а також за розкриття своїх резервних копій.
- Про втрачені або вкрадені пристрої BYOD слід повідомити в службу підтримки IT або відділ інформаційної безпеки протягом максимум 24 годин.
- Пристрої BYOD можна дистанційно стерти, як правило, за згодою власника, коли він/вона повідомляє, що його/її пристрій є вразливим/зараженим або втраченим/викраденим, або його/її звільняють з роботи. Подібним чином пристрої BYOD можуть бути віддалено стерті без згоди власника, якщо IT-спеціалісти підозрюють або виявляють порушення даних чи політики, загрозу зловмисного програмного забезпечення чи вірусу або атаку, розпочату на/через пристрій.
- Щоб зберегти конфіденційність користувачів BYOD і уникнути доступу керівництва організації до особистої інформації на пристроях, користувачам BYOD рекомендується відокремити особисті дані від робочих даних в окремих папках/каталогах на своїх пристроях за допомогою ідентифікаторів.

Після того, як користувач погодився з BYOD політикою компанії, а системні адміністратори, або служба підтримки переконались в тому, що пристрій відповідає вимогам, необхідно встановити UEM [25].

Розгортання BYOD політики за допомогою Endpoint Central від ManageEngine:

Зважаючи на постійне зростання кількості постачальників атак і частоти атак, необхідно цілодобово підтримувати всі кінцеві точки вашого підприємства в

актуальному стані та виправляти їх. Функція автоматичного розгортання виправлень (APD) Endpoint Central надає системним адміністраторам можливість автоматично розгортати виправлення, яких немає на їхніх мережевих комп'ютерах, без ручного втручання.

Через вкладку "Patch Management" необхідно перевірити, чи всі необхідні компоненти встановлені, якщо ні – встановити.

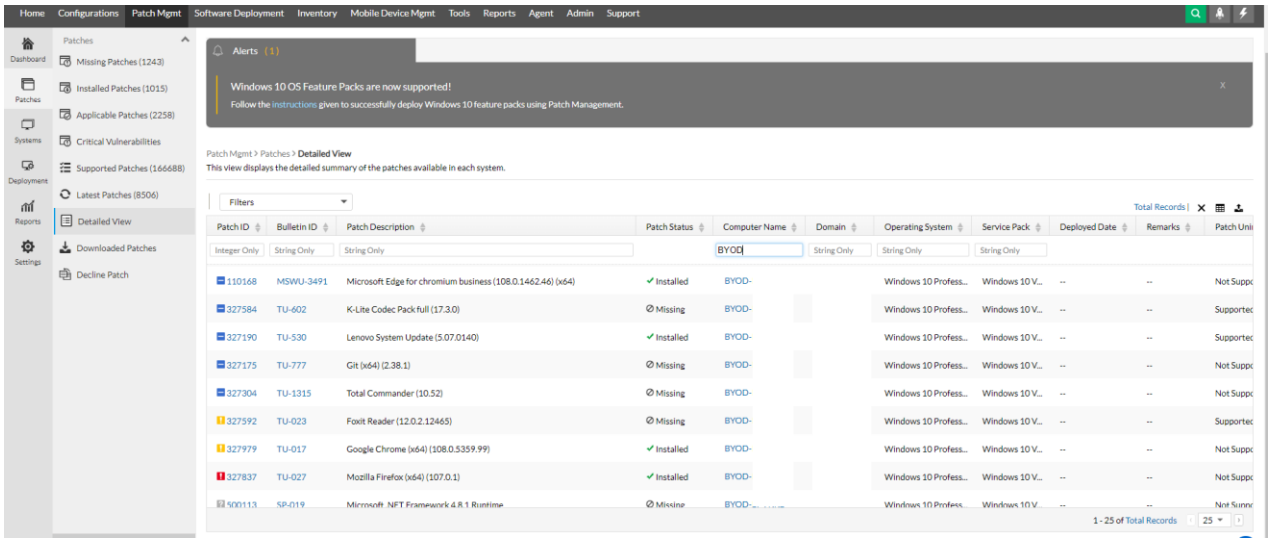


Рис.3.1. Встановлення необхідних компонентів через "Patch Management"

Для налаштування робити пристроїв необхідно визначити програмне забезпечення, яке має бути встановлене. За допомогою вкладки "Software Deployment" визначаємо список ПЗ, що має бути встановлений на пристрій, відповідно до ролі користувача, а також операційної системи.

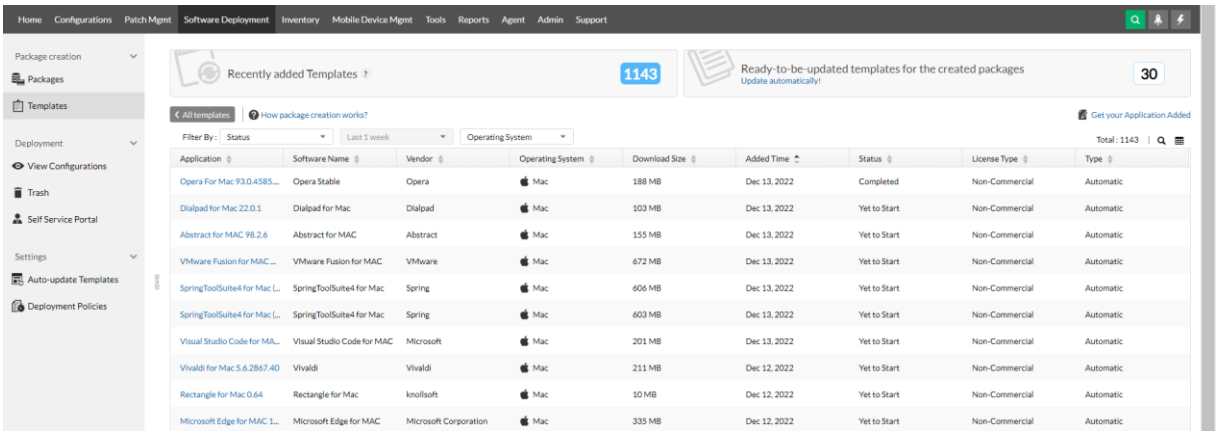


Рис.3.2. Встановлення програмного забезпечення

Окрім цього необхідно визначити список програмного забезпечення, яке заборонено в компанії, також можна додати версію яку буде заборонено встановлювати через виявлені вразливості.

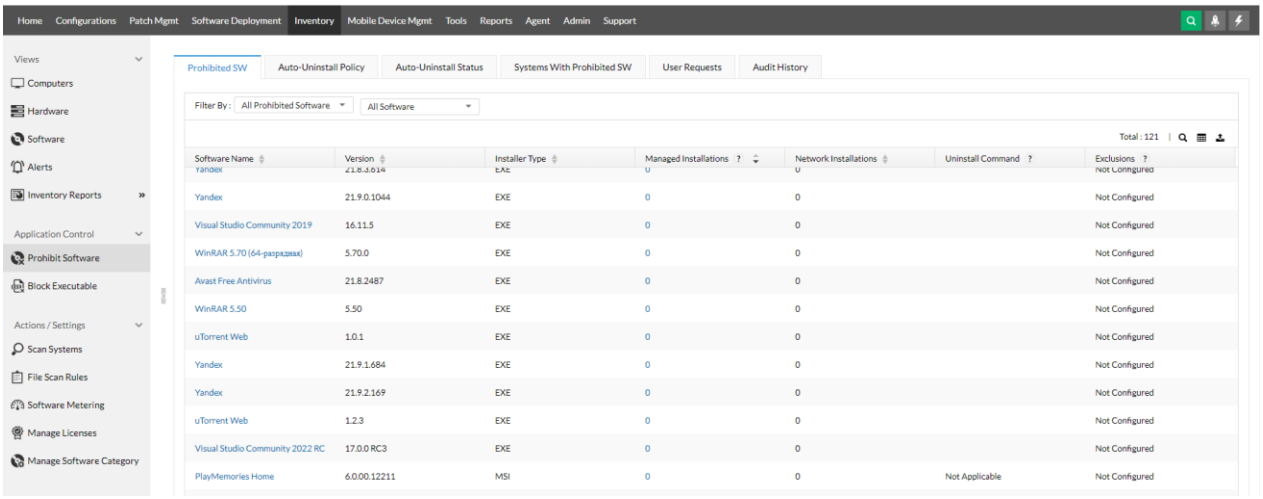


Рис.3.3. Визначення забороненого програмного забезпечення

Для того, щоб відокремити особисті дані від робочих даних необхідно перейти на вкладку “Inventory” та вибрати необхідний аккаунт, який використовуються в робочих цілях. Це необхідно для того, щоб застосувати політики тільки на один аккаунт, не впроваджуючи їх на персональний аккаунт користувача.

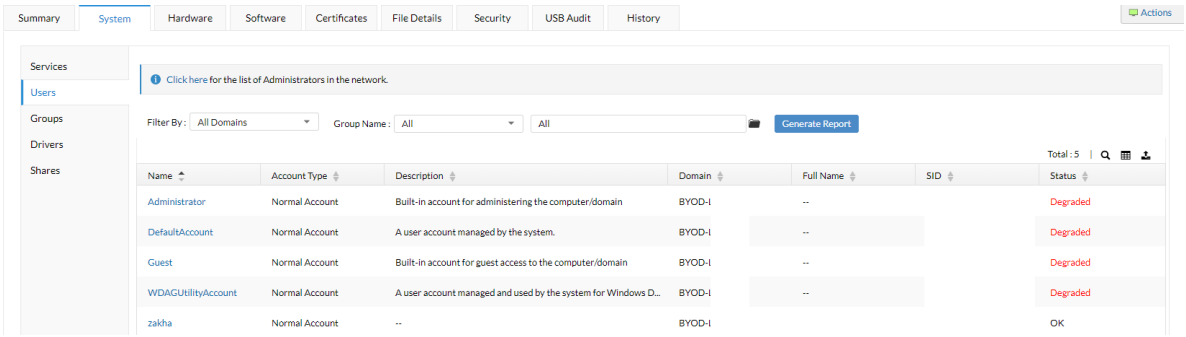
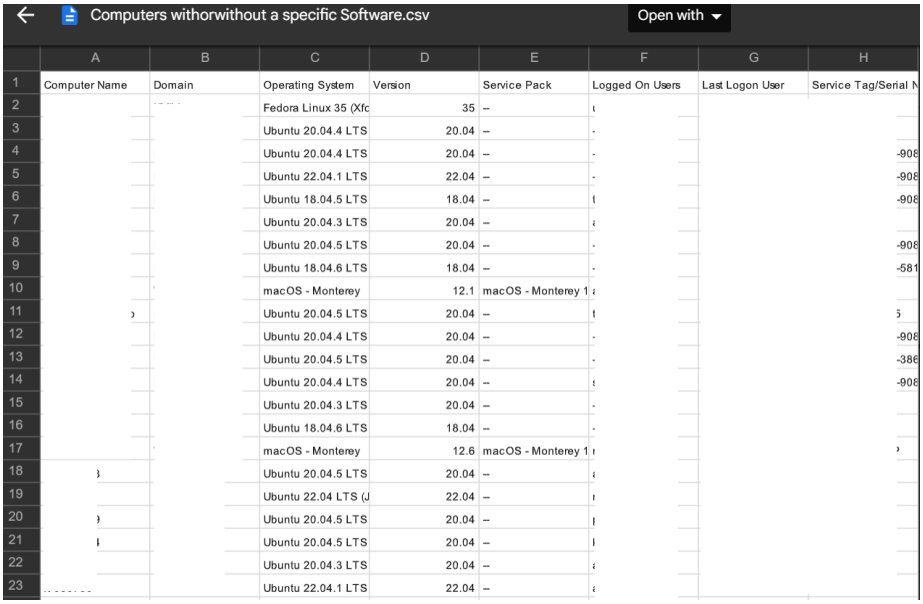


Рис.3.4. Вибір робочого акаунту для застосування політик

Окрім цього, треба налаштувати репорти, для того, щоб контролювати всі пристрої на яких встановлене рішення. Наприклад, є можливість того, що користувач випадково видалить «агент» зі свого акаунта, тим самим ніякі політики більш не будуть застосовуватись. Для цього необхідно налаштувати репорт «Комп`ютери

без спеціального програмного забезпечення». Тим самим системні адміністратори завжди будуть в курсі, на яких пристроях відсутнє певне програмне забезпечення.


Computers withorwithout a specific Software.csv

Open with

	A	B	C	D	E	F	G	H
1	Computer Name	Domain	Operating System	Version	Service Pack	Logged On Users	Last Logon User	Service Tag/Serial N
2			Fedora Linux 35 (Xfc	35	--			
3			Ubuntu 20.04.4 LTS	20.04	--			
4			Ubuntu 20.04.4 LTS	20.04	--			-908
5			Ubuntu 22.04.1 LTS	22.04	--			-908
6			Ubuntu 18.04.5 LTS	18.04	--			-908
7			Ubuntu 20.04.3 LTS	20.04	--			
8			Ubuntu 20.04.5 LTS	20.04	--			-908
9			Ubuntu 18.04.6 LTS	18.04	--			-581
10			macOS - Monterey	12.1	macOS - Monterey 1			
11			Ubuntu 20.04.5 LTS	20.04	--			
12			Ubuntu 20.04.4 LTS	20.04	--			-908
13			Ubuntu 20.04.5 LTS	20.04	--			-386
14			Ubuntu 20.04.4 LTS	20.04	--			-908
15			Ubuntu 20.04.3 LTS	20.04	--			
16			Ubuntu 18.04.6 LTS	18.04	--			
17			macOS - Monterey	12.6	macOS - Monterey 1			
18			Ubuntu 20.04.5 LTS	20.04	--			
19			Ubuntu 22.04 LTS (J	22.04	--			
20			Ubuntu 20.04.5 LTS	20.04	--			
21			Ubuntu 20.04.5 LTS	20.04	--			
22			Ubuntu 20.04.3 LTS	20.04	--			
23			Ubuntu 22.04.1 LTS	22.04	--			

Рис. 3.5. Приклад звіту

3.2. Розроблення рекомендацій щодо технології управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD

Існує велика різноманітність мобільних пристроїв, і функції безпеки, доступні для цих пристроїв, також дуже відрізняються. Деякі пристрої пропонують лише кілька основних функцій, тоді як інші пропонують складні функції. Це не обов’язково означає, що більше функцій безпеки – краще; насправді багато пристроїв пропонують більше функцій безпеки, тому що можливості, які вони надають, роблять їх більш сприйнятливими до атак, ніж пристрої без цих можливостей. Різноманітність функцій безпеки робить неможливим створення конкретних рекомендацій, які стосуватимуться всіх мобільних пристроїв і дотримуватися їхніх рекомендацій щодо безпеки. Загальні рекомендації такі:

Організація повинна:

- Встановити програмне забезпечення для керування мобільними пристроями (UEM) або програмне забезпечення для дистанційного керування та моніторингу

(RMM) (включно з антивірусними програмами/програмами захисту від зловмисного програмного забезпечення, де це можливо) на особистих пристроях співробітників. Це програмне забезпечення дозволить авторизованому IT-персоналу отримувати доступ, керувати, контролювати та віддалено видаляти всю інформацію, пов’язану з компанією, включаючи календарі, електронну пошту та інші програми. Це особливо важливо, коли пристрій втрачено, викрадено або виведено з експлуатації.

- Переконатись, що пристрій належним чином налаштовано відповідно до стандартів безпеки та, якщо необхідно, змінити параметри відповідно до вимог безпеки компанії.

- Переконатись, що всі оновлення програмного/апаратного забезпечення та виправлення успішно застосовано.

- Просканувати пристрій на наявність неавторизованих або небезпечних програм і видалити їх.

- Перевірити, чи дотримуються стандарти політики контролю доступу компанії.

- Контролювати пристрій і будь-які ресурси компанії, до яких він підключається.

Працівник повинен:

- Використовувати надійний пароль і автоматичне блокування пристроя відповідно до політики контролю доступу унастанови.

- Співпрацювати з IT-персоналом, щоб переконатися, що на пристроях і всьому трафіку до/від пристрою діє відповідна технологія шифрування.

- Ретельно дотримуватись політики цифрового зв’язку та бути обережними, відкриваючи електронні листи та/або вкладення на пристрої.

- У будь-який час утримуватись від відео- чи аудіозапису будь-де в будівлі або на території компанії, якщо це не дозволено заздалегідь керівником.

- Підтримувати пристрій у вихідному стані, не модифікуючи його операційну систему або не зламуючи пристрій, щоб обійти вбудовані функції безпеки та протоколи.

- Не завантажувати програми чи програмне забезпечення з неавторизованих джерел.

- Не навмисно чи навмисно завантажувати та не передавати конфіденційні бізнес-дані на пристрій.

- Повідомляти керівника і/або ІТ-департамент про будь-який втрачений чи викрадений пристрій або про несанкціонований доступ.

- Цілком дотримуватись політики компанії щодо прийнятного використання технологій, безпеки мобільних пристроїв і контролю доступу [2].

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми управління мобільними користувачами в корпоративній інформаційній системі з використанням концепції BYOD.

Проаналізовано ризики безпеки спричинені BYOD на корпоративну інформаційну систему. Визначено основні рішення для створення системи безпеки політики BYOD.

Визначено існуючі методи управління мобільними користувачами концепції BYOD.

Встановлено основні призначення, можливості та функції управління мобільними користувачами на основі Unified Endpoint Management. Досліджено рішення Unified Endpoint Management від ManageEngine. Розглянуто архітектуру рішення та основних компонентів.

У роботі запропоновано варіант управління мобільними користувачами, для цього було розглянуто приклад робочої системи Unified Endpoint Management від ManageEngine.

Розроблено рекомендації щодо технології управління мобільними користувачами корпоративної інформаційної системи з використанням концепції BYOD.

ПЕРЕЛІК ПОСИЛАНЬ

1. Legal Issues in Secure Implementation of Bring Your Own Device. URL: https://www.researchgate.net/publication/301234173_Legal_Issues_in_Secure_Implementation_of_Bring_Your_Own_Device_BYOD
2. Device Security Guidance. URL: https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
3. THE INFLUENCE OF BYOD SECURITY RISK ON SME INFORMATION SECURITY EFFECTIVENESS. URL: https://www.proquest.com/openview/d65e71e7177f44fb0f5603dd92f4798d/1?pq-origsite=gscholar&cbl=18750&diss=y
4. Exploring information systems security implications posed by BYOD for a financial services firm. URL: https://journals.sagepub.com/doi/full/10.1177/02663821211036400
5. Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory. URL: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1051&context=jmwais
6. BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY. URL: https://researchrepository.murdoch.edu.au/id/eprint/25699/1/bring_your_own_device.pdf
7. Risk Management in the Era of BYOD. URL: https://cups.cs.cmu.edu/soups/2013/risk/Yang-RP-IT-2013.pdf
8. Enterprise Mobile Device Management Requirements and Features. URL: https://ieeexplore.ieee.org/document/9162763
9. Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9199866

10. An overview of endpoint management challenges and the available solutions. URL:https://download.manageengine.com/products/desktop-central/desktop-management-whitepaper.pdf

11. Leveraging BYOD. URL:https://download.manageengine.com/products/desktop-central/leveragingbyod.

12. Unified Endpoint Management Software for a Small Company. URL:https://www.theseus.fi/bitstream/handle/10024/510474/Schafer_Jarrod.pdf?sequence=2&isAllowed=y

13. User's Guide to Telework and Bring Your Own Device (BYOD) Security. URL:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

14. The need for Unified Endpoint Management (UEM). URL:https://www.manageengine.com/products/desktop-central/unified-endpoint-management-solutions.html

15. Software Deployment: Features and Capabilities. URL:https://www.manageengine.com/products/desktop-central/windows-software-installation.html?uem

16. Emerging Tech: What is Unified Endpoint Management (UEM). URL:https://www.computer.org/ublications/tech-news/trends/what-is-unified-endpoint-management

17. What is UEM - unified endpoint management? URL:https://www.ibm.com/topics/uem

18. Endpoint Device Management in the BYOD Era. URL:https://www.quest.com/community/blogs/b/unified-endpoint-management/posts/endpoint-device-management-in-the-byod-era

19. BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts. URL:https://www.tandfonline.com/doi/abs/10.1080/10919392.2022.2028530

20. What is Unified Endpoint Management (UEM)? URL:https://www.techtarget.com/searchenterprisedesktop/definition/unified-endpoint-management-UEM

21. Endpoint Central MSP's patch management process. URL:https://www.manageengine.com/desktop-management-msp/patch-management.html

22. Managing and Securing the Internet of Things. URL:https://www.solutionspt.com/blackberry-uem

23. What Is Unified Endpoint Management (UEM) And How Does It Work? URL:https://expertinsights.com/insights/what-is-unified-endpoint-management-uem-and-how-does-it-work/

24. Threats Introduced by Bring Your Own Devices (BYOD) Adoption in an Ethiopian Higher Educational Institution: Solutions to Security and Privacy. URL:https://www.proquest.com/openview/d07970c0a0abb9fb7c67c18631c93bad/1?pq-origsite=gscholar&cbl=2029987

25. ISO 27001 COMPLIANT MANAGEMENT OF MOBILE DEVICES IN A MEDIUM SIZE PRIVATE ENTERPRISE. URL:https://info-savvy.com/iso-27001-annex-a-6-2-mobile-devices-and-teleworking/

26. 7 Essential Features for Mobile Device Management (MDM) Solutions. URL:https://solutionsreview.com/mobile-device-management/7-essential-features-for-mobile-device-management-mdm-solutions/

27. Magic Quadrant for Unified Endpoint Management Tools. URL:https://www.gartner.com/doc/reprints?id=1-2AOMHDK6&ct=220727&st=sb

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APWG – (Anti-Phishing Working Group,

BEC –

BYOD – Bring-Your-Own-Device

CASB – Cloud Access Security Broker

CSP – Cloud Service Provider

DEM – Digital Experience Monitoring

DMZs – Demilitarized Zones

DNS – Domain Name System

DTLS – Datagram Transport Layer Security

IaaS – Infrastructure as a Service

NAC – Network Access Control

NGFW – Next-Generation Firewall

PaaS – Platform as a Service

POPs – Points Of Presence

SASE – Secure Access Service Edge

SDN Software Defined Network

SDP – Software Defined Perimeter

SD-WAN – Software-Defined Wide Area Network

SIEM – Security Information and Event Monitoring

SSE – Cloud-Delivered Security Service Edge

TIC – Trusted Internet Connections

VPN – Virtual Private Network

WFA – Work-From-Anywhere

ZT – Zero Trust

ZTA – Zero Trust Architecture

ZTNA – Zero Trust Network Acces

ВСТУП

Актуальність дослідження. Підхід до забезпечення безпеки, який передбачав, що додатки та користувачі перебувають у периметрі мережі організації, вже не відповідає дійсності. Сьогодні корпоративні дані переміщуються в хмару, співробітники все частіше працюють віддалено, а ініціативи з цифрової трансформації вимагають від фахівців з IT та кібербезпеки спритності, щоб використовувати нові бізнес-можливості.

У результаті традиційний периметр мережі розпадається, що визначає потребу в нових моделях контролю доступу, захисту даних і протидії загрозам. У світлі цих змін організації виявляють, що їхня існуюча колекція автономних точкових продуктів, таких як брандмауери, захищений веб-шлюз, засоби запобігання втраті даних (DLP) і брокери безпеки доступу до хмари (CASB), більше не можна використовувати в хмарі.

Технологія Secure Access Service Edge (SASE) забезпечує конвергентну мережу та безпеку як послугу. Вона об’єднує мережеві служби та служби безпеки в хмарну архітектуру для захисту користувачів, додатків і даних у будь-якому місці. Враховуючи, що користувачі та додатки більше не знаходяться в корпоративній мережі, заходи безпеки не можуть залежати від звичайних апаратних пристроїв на периметрі мережі.

Натомість технологія SASE забезпечує необхідну мережу та безпеку як хмарні послуги. При правильному виконанні модель SASE виключає пристрої, що базуються на периметрі, та застарілі рішення. Замість того, щоб передавати трафік на пристрій для забезпечення безпеки, користувачі підключаються до хмарної служби SASE, щоб безпечно використовувати додатки та дані з послідовним дотриманням політики безпеки.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE.

Об'єкт дослідження – забезпечення безпечної роботи гібридних працівників організації.

Предмет дослідження – технологія забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE.

Мета роботи – розробити порядок застосування технології забезпечення безпечної роботи гібридних працівників організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення безпечної роботи гібридних працівників організації;

проаналізувати підходи до забезпечення безпечної роботи гібридних працівників організації;

проаналізувати існуючі рішення із забезпечення безпечної роботи гібридних працівників організації;

проаналізувати методи та засоби забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE;

розкрити порядок реалізації технології забезпечення безпечної роботи гібридних працівників організації.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології забезпечення безпечної роботи гібридних працівників організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми захисту організацій від фішингових атак від фішингових атак

Фішинг вже багато років є однією з найпопулярніших хакерських (шахрайських) атак, яка є формою соціальної інженерії. Такий вид атаки передбачає собою обман та психологічну маніпуляцію з боку кіберзлочинців. Використання перевірених джерел, таких як лист на корпоративну електронну пошту, дзвінок від знайомої людини (родичі, друзі або ж навіть ваш керівник з роботи) та інше, суб'єкти загрози маскуються та спонукають користувачів (фактично своїх жертв) виконувати певні дії. Таким чином вони змушують людину надавати персональні дані, доступи до закритої інформації, як от банківський рахунок та дані кредитної картки, паролі та доступи до інших важливих та захищений джерел інформації, встановлення шкідлих файлів (які можуть бути націлені як на збір даних так і на шпигунство, виведення з ладу пристрої, а то і всієї захищеної мережі в цілому). З кожним роком тенденція використання фішингової атаки на електронну пошту постійно зростає як це проілюстровано на рис. 1.1, а й набуває змін і впроваджує нові способи впливу.

Для подальшого аналізу проблеми захисту від фішингових атак було використано дані, що зібрані робочою групою по боротьбі з фішингом (Anti-Phishing Working Group, APWG), яка є міжнародною коаліцією, некомерційною галузевою асоціацією та зосереджена на усуненні крадіжки особистих даних і шахрайства, які є результатом зростаючої проблеми фішингу [1].

Основні завдання які виконує APWG полягають у наступному:

- Унікальні фішингові сайти, що є основним показником кількості повідомлень про фішинг у всьому світі.

- Унікальні теми фішингових електронних листів, де враховуються листи-приманки, які містять різні теми електронних листів.

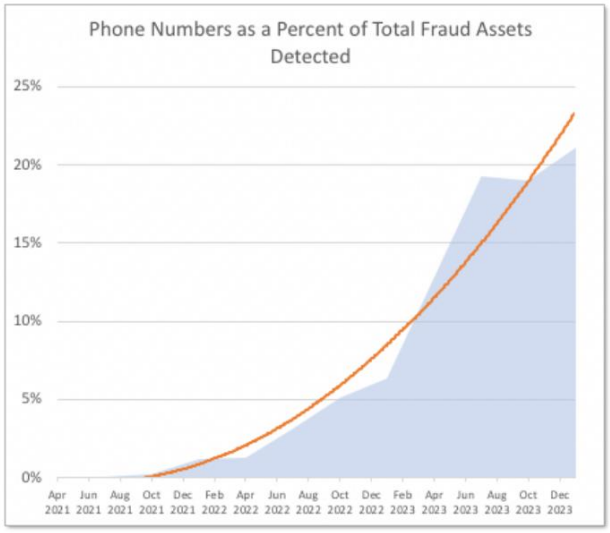


Рис 1.1. Тенденція збільшення фішингових атак [5]

- Збір даних щодо кількості атакованих брендів шляхом вивчення звітів про фішинг і нормалізації написання назв брендів.

Згідно зі звітом за 1квартал 2023 [1], APWG зафіксувала:

- 1 624 144 фішингових атак, серед яких одним з найпопулярніших для кібератак направлень залишається фінансовий сектор, на який припало 23,5% від всіх атак, що менше на 4% порівняно з 2022 роком;
- фішинг націлений на криптовалюту падає до 2% через хвилювання які відбувались у криптоіндустрії через крах FTX у листопаді 2022 року;
- спостерігалося зростання обсягу фішингових або вішингових повідомлень голосової пошти на більше ніж 40%, якщо порівнювати з показниками за 2022 рік.

Аналіз айбільш популярних секторів для фішингових атак за 1 квартал 2023 року показав, що другим для популярності сектором для атаки стали послуги надання програмного забезпечення (SAAS), що становить 18,8% від загальної

кількостфі атак, атаки на компанії соціальних мереж заняли третє місце у списку і складає 18,2% атак (рис.1.2).

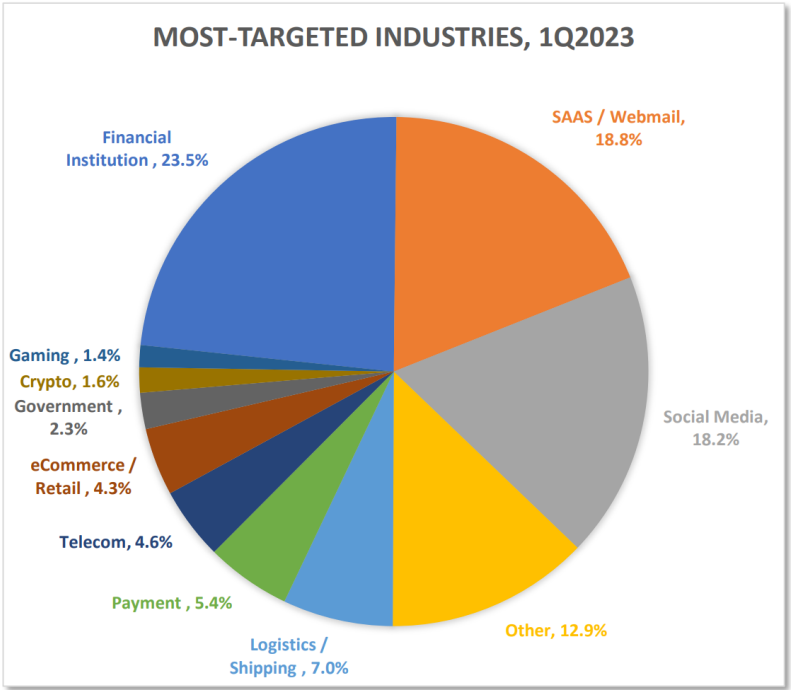


Рис.1.2. Найбільш популярні сектори для фішингових атак за 1 квартал 2023 року

Згідно зі звітом за 2 квартал 2023 [2] APWG зафіксувала:

- 1 286 208 фішингових атак, що стало третім показником за величиною кількості атак за квартал;
- фінансовий сектор залишається найбільш атакованим – 23,5% атак. Також зафіксовано що в загальному атаки були здійснені на банківські грошові перекази, де сума середнього банківського переказу становила 293 359 доларів США, а це на 57% більше в порівнянні з середніми сумами (не менш ніж 187 053 доларів) за перший квартал. А от обсяг атак впав до 29%, з чого можна зробити висновки, що зловмисники поступилися кількістю атак заради більшої наживи;
- найпопулярнішим шахрайством стали авансові комісії як метод виводу готівки – 44% від загальної кількості. Тобто задля виводу грошей злочинці просили, наприклад, подарункові карти популярних платформ (Amazon, Apple Store) замість звичайної оплати на банківський рахунок – 34% випадків;

- з’явився гібридний вид атаки – вішинг або ж так званий голосовий фішинг (5%). Атака працює наступним чином: жертва атаки отримує електронного листа де зазначено що було списано кошти за оплату товару чи якоїсь послуги і щоб скасувати оплату та отримати відшкодування необхідно зателефонувати за вказаним в листі номером. В таких листах задля довіри викокористовували такі бренди як PayPal Geek Squad, McAfee та інші;
- кількість унікальних тем для атак виконаних електронною поштою зменшилася майже в два рази, оскільки в середньому за перший квартал 2023 року показник становив понад 40 000 на місяць (рис.1.3)

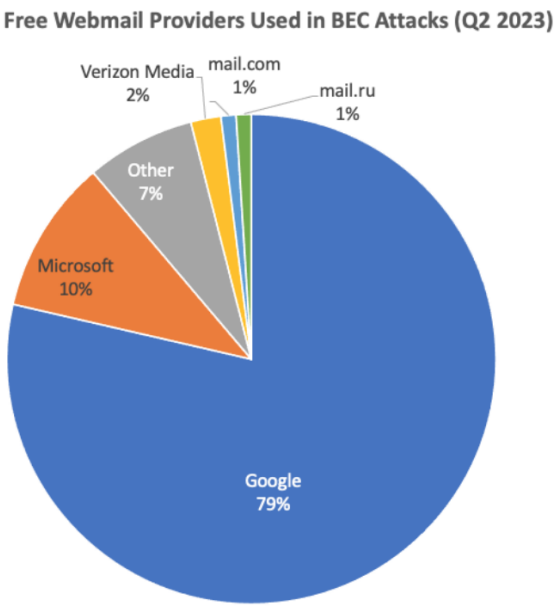


Рис. 1.3. Безкоштовні поштові сервіси які використовувалися в BEC-атаках [2]

Згідно з рис.1.4. фінансовий сектор на першому місці 2023 року - 23,5% від усіх атак, друге місце посідає кількість атак на компанії соціальних мереж – 22,3%, а третє атаки стали послуги надання програмного забезпечення (SAAS/Webmail), що становить 16,3%.

Згідно зі звітом за 3 квартал 2023 [3]:

- зафіксовано 999 956 фішингових атак, що на 37,5% менше в порівнянні з 1 кварталом 2023 року, фактично фішинг впав до рівня який спостерігався в кінці 2021 року;

- підкатегорія атак на голосову пошту фішинг/вішинг зросла до 40% вродовж 1-3 кварталів 2023 року;

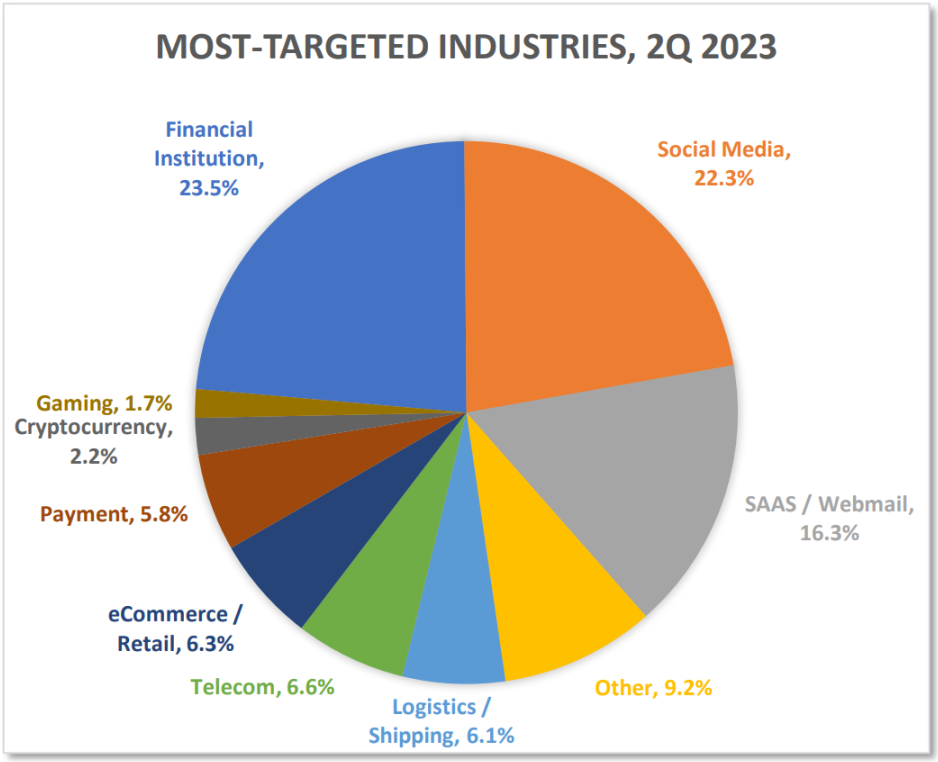


Рис. 1.4. Найбільш популярні сектори для фішингових атак за 2 квартал 2023 року

- атака на перекази банківських коштів в загальному припадала на середню суму в 164 645 доларів США, тобто середній показник впав на 44% порівняно з 2 кварталом 2023 року, що станов 293 359 доларів США;

- обсяг атак BEC на банківські перекази зріс на 55%;

- кількість унікальних тем для електронної пошти стабілізувалася на рівні близько 32 000 після середнього рівня понад 40 000 на місяць у першому кварталі 2023 року;

- виявлено 250 унікальних телефонних номерів, що використовувалися для гібридної вішингової атаки, які видавали себе за 15 різних брендів під час гібридних атак вішингу за 3 квартал;

- рекордно високий щодо атак квартал, який підтвердив, що не зважаючи на падіння показників у попередніх роках, фішинг знову піднявся рівня атак який спостерігався у 2021 році.

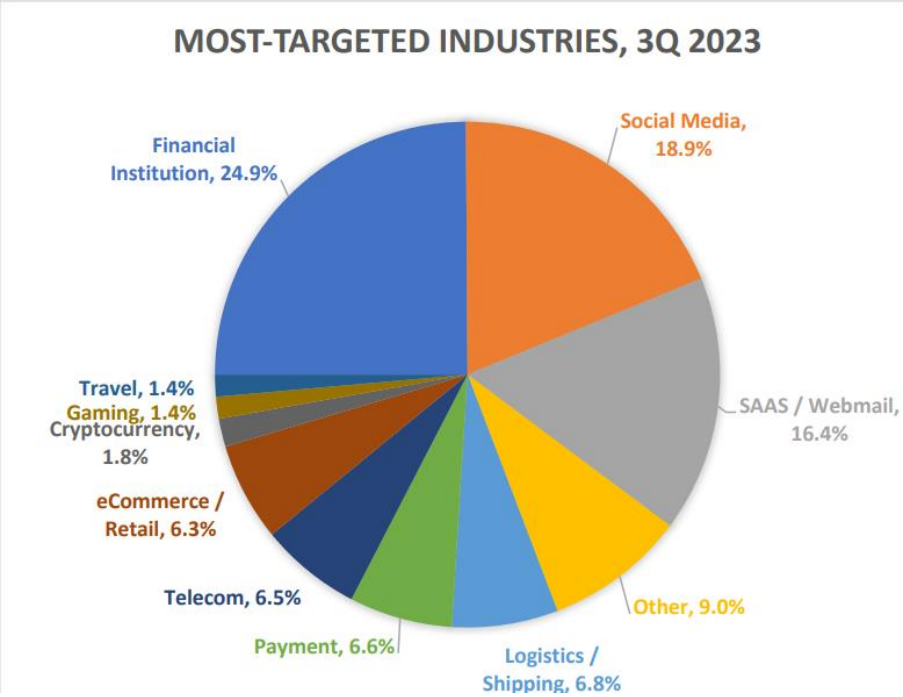


Рис. 1.5. Найбільш популярні сектори для фішингових атак за 3 квартал 2023 року

Фінансовий сектор залишається найбільш атакованим – 24,9% від усіх атак, друге місце посідають атаки на соціальні мережі – 18,9%, а третє місце зайняли SAAS/Webmail атаки -16,4%.

Також цього кварталу спосткрігалося що 79% BEC атак використовували безкоштовний домен веб-пошти, що менше на 8% порівняно з попереднім кварталом. Решта 21% BEC атак використовували зловмисно зареєстровані домени та скомпрометовані облікові записи електронної пошти, де Google став найпопулярнішим провайдером веб-пошти серед кіберзлочинців адреси Gmail становили 84% облікових записів веб-пошти шахраїв.

Отримання грошей через подарункові картки також залишається популярною атакою, де найчастіше вимагали картки Amazon і Apple Store.

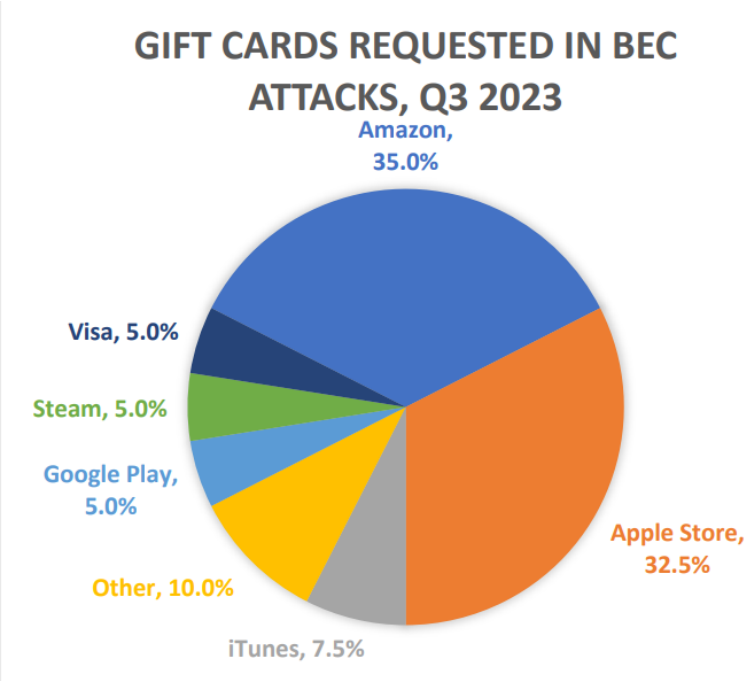


Рис. 1.6. Запити на подарункові карти у BEC атаках

Згідно зі звітом за 4 квартал 2023 [4]:

- Зафіксовано 1 077 501 фішинг-атак, у підсумку це близько п’яти мільйонів (4 987 809) фішинг-атак за весь 2023 рік, через що він вважається найгіршим роком для фішингу в історії перейшовши планку яка була зафіксована у 2022 році з кількістю атак у 4,7 мільйона
- Атаки за 4 квартал 2023 року стали найнижчим зафіксованм показником, оскільтки їх кількість частково скоротилася через закриття програми безкоштовного доменного імені Freenom. Цей безкоштовній сервіс видавав домени рівня .TK, .ML, .GA, .CF і .GQ і використовувся злочинцями на протязі багатьох років. Фактично через цей сервіс виконувалися 14% атак у всьому світі і 60% фішингових доменів про які повідомлялося ще у 2022. Проте у січні 2023 Freenom припинили безкоштовну реєстрацію доменів, а пізніше взагалі оголосили про повний вихід з бізнесу доменними іменами.
- Кількість унікальних тем у електронних листах трохи впала, проте загальна кількість таких повідомлень залишається на одному рівні в порівнянні з попередніми кварталами.

- Різкий зріст кількості атак на платформи соціальних мереж, що склало 42,8% від всіх фішингових атак.
- Фішинг за допомогою телефонних дзвінків (голосовий фішинг або «вішинг») зростає з кожним кварталом.
- Кількість нападів на банківські перекази теж зростає, але середня сума на яку скорюється атака знизилася до 56 195 доларів США, і це не зважаючи на те, що кількість банківських перевірок зросла на 24%.
- Шахрайство з подпрунковими картками було найпопулярнішим й становило 37,6%. Далі за популярністю йдуть випадки шахрайства з авансовою комісією – 30,6%, перенарахування заробітної плати - 9,2%.
- Найпопулярніші початальники безкоштовної веб-пошти через які кіберзлочинці скоюють атаки: Google – 52%, Microsoft - 21%, Apple – 20%

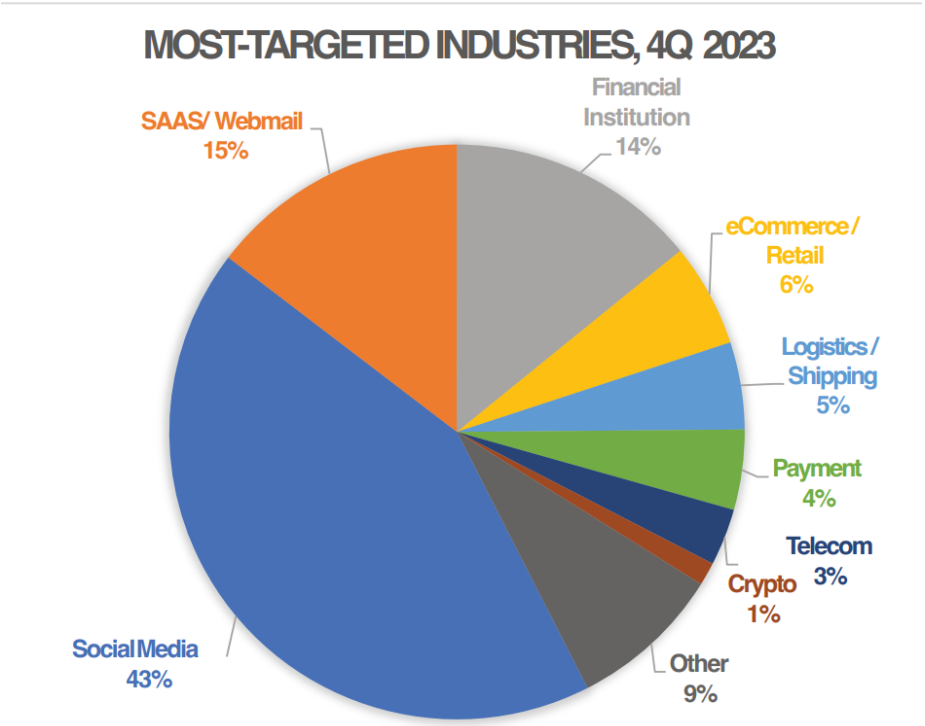


Рис. Найбільш популярні сектори для фішингових атак за 4 квартал 2023 року

Перше місце згідно з рис. посіли фішингові атаки наплатформи соціальних медіа – 42,8% від всіх атак, що є різким стрибком в показниках в порівнянні з 18,9% атак за 3 квартал 2023 року. Друге місце отримав сектор SAAS/Webmail атаки –

15%, а фінансовий сектор, який стабільно тримався на першому місці, в цей раз посідає третє отримавши 14% від усіх атак порівняно з показником у 24,9% за попередній квартал.

Отже для організацій важливим питання є захист від фішингових атак, що дозволить зазистити інформаційні ресурси організації.

1.2. Аналіз підходів до захисту інформаційних ресурсів організацій від фішингових атак

Згідно зі звітом APWG за 1-й квартал 2024 року [5]:

- Зафіксовано лише 963 994 фішингових атак, що в свою чергу стало найнижчим показником із 4-го кварталу 2021 року
- Кількість отриманих звітів зменшилася, проте кількість унікальних кампаній створених за допомогою електронної пошти зросла на 64% порівняно з 4-им кварталом 2023 року, що свідчить про те, що кіберзлочинці урізноманітнювали рядки тем своїх електронних листів, щоб обійти розроблену фільтрацію електронної пошти

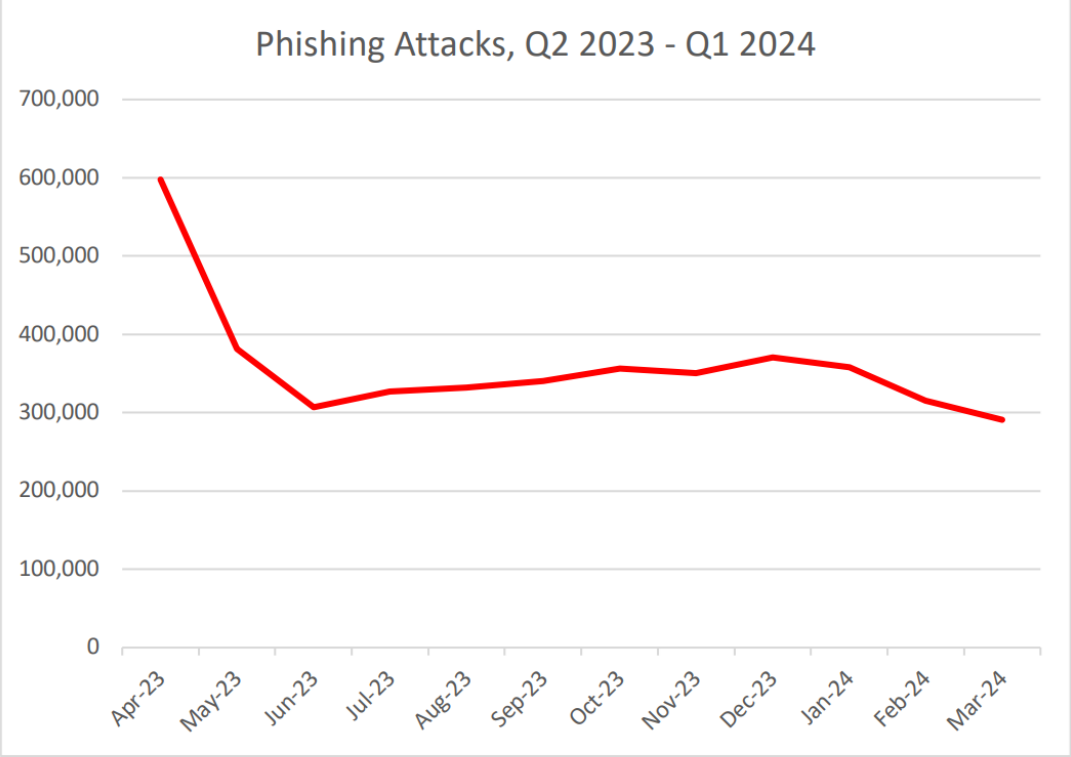


Рис. Фішингові атаки, кв.2 2023 – кв.1 2024 [5]

- Телефонний фішин поширюється безконтрольно. Номери телефонівикористані для фішингу становили понад 20% пов’язаних із шахрайством активів
- Фішинг за допомогою телефонних дзвінків — так званий голосовий фішинг або «вішинг» постійно збільшується з кожним кварталом

- Середня сума банківського переказу, яка була атакована кіберзлочинцями становила 84 059 доларів США, тобто показник зріс майже на 50% в порівнянні з показником за попередній квартал

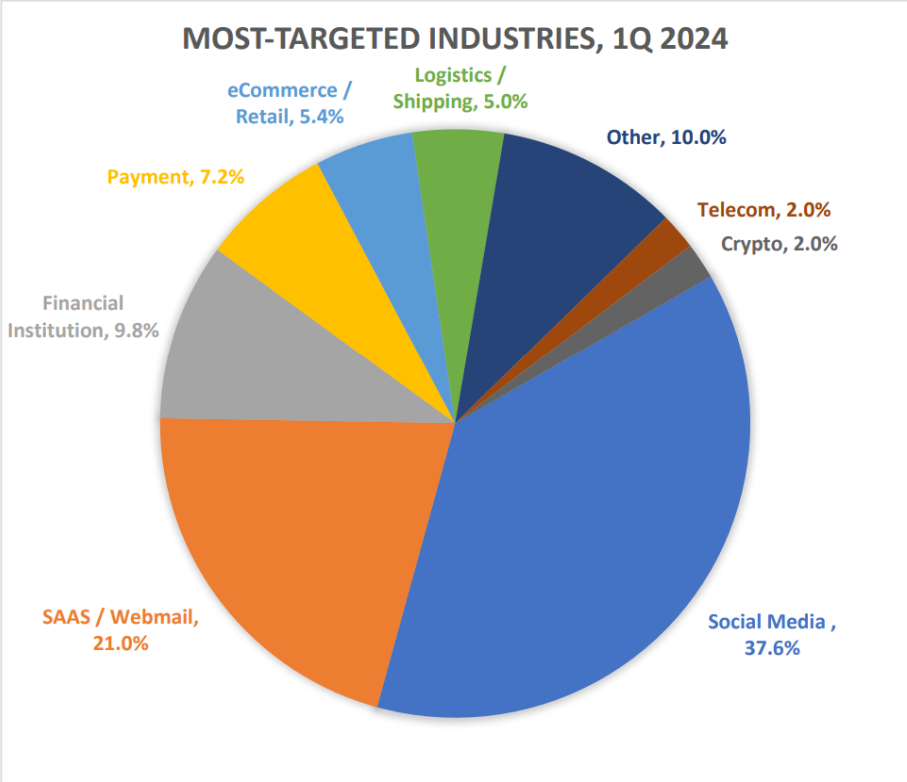


Рис. Найбільш популярні сектори для фішингових атак за 1 квартал 2024 року

Платформи соціальних медіа залишаються найбільш атакованим сектором - 37,4%. Друге місце сектор SAAS/Webmail – 21%, а третє знову отримав банківський сектор – 9,8%

ВИСНОВКИ

В роботі проведено дослідження проблеми забезпечення безпечної роботи гібридних працівників організації, визначено його мету та завдання.

Проведено аналіз існуючих технологій забезпечення безпечної роботи гібридних працівників організації. Технологія Secure Access Service Edge (SASE) забезпечує конвергентну мережу та безпеку як послугу. Вона об’єднує мережеві служби та служби безпеки в хмарну архітектуру для захисту користувачів, додатків і даних у будь-якому місці.

Досліджено методи та засоби забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE. Визначено призначення, основні функції та склад рішення FortiSASE.

Рішення FortiSASE має захищений веб-шлюз на основі штучного інтелекту, забезпечує доступ до мережі з нульовою довірою, застосовує брокер безпеки доступу до хмари, реалізує брандмауер як послугу та використовує захищену програмно-конфігуровану розподілену мережу під керуванням єдиної операційної системи за допомогою однієї консолі.

На основі досліджень проведених в роботі запропоновано порядок застосування технології забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE.

За допомогою рішення FortiSASE реалізується архітектура SASE (FWaaS, SWG, ZTNA) для забезпечення безпечного доступу віддалених користувачів у таких випадках:

захищений доступ до Інтернету (SIA), коли користувачі отримують доступ до Інтернету та веб-додатків;

безпечний приватний доступ (SPA), коли користувачі отримують доступ до приватних корпоративних додатків, захищених FortiGate NGFW;

захищений доступ SaaS (SSA), коли користувачі отримують доступ до додатків SaaS.

Функції безпеки можна налаштувати та пропонується багато налаштувань, які можна побачити на FortiGate. FortiSASE пропонує такі режими як кінцева точка та безпечний веб-шлюз (SWG), які були розглянуто в даній роботі.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології забезпечення безпечної роботи гібридних працівників організації.

Таким чином, правильна реалізація технології забезпечення безпечної роботи гібридних працівників організації має сприяти ефективному захисту корпоративних інформаційних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lawrence Miller. Single-Vendor SASE For Dummies. Fortinet Special Edition. John Wiley & Sons, Inc. 2023. URL: https://www.fortinet.com/content/dam/fortinet/assets/ebook/single-vendor-sase-for-dummies.pdf (дата звернення: 26.11.2023).

2. Hybrid Security Trends 2023. Netwrix Research Lab. URL: https://www.netwrix.com/download/collaterals/Netwrix_Hybrid_Security_Trends_Report_2023.pdf (дата звернення: 26.11.2023).

3. 2023 Global Networking Trends Report. Cisco. URL: https://www.cisco.com/c/en_uk/solutions/enterprise-networks/xa-09-2023-networking-report.html (дата звернення: 26.11.2023).

4. Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly. Zero Trust Architecture. NIST Special Publication 800-207: https://doi.org/10.6028/NIST.SP.800-207 (дата звернення: 26.11.2023).

5. Jonathan Forest, Naresh Singh, Andrew Lerner, Karen Brown. Magic Quadrant for SD-WAN. Gartner. 27 September 2023 - ID G00778908 URL: https://www.gartner.com/doc/reprints?id=1-2F73TM21&ct=231003&st=sb (дата звернення: 26.11.2023).

6. Andrew Lerner, Jonathan Forest, Neil MacDonald, Nat Smith, Charlie Winckless. Magic Quadrant for Single-Vendor SASE. Gartner. 16 August 2023 - ID G00785023. URL: https://www.gartner.com/doc/reprints?id=1-2ERFQZGF&ct=230821&st=sb (дата звернення: 26.11.2023).

7. Universal SASE: Comprehensive, Single-Vendor SASE for Securing the Hybrid Workforce. Solution Brief. Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortisase-cloud-delivered-securtiy-to-every-user.pdf (дата звернення: 26.11.2023).

8. SASE Architecture. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/sase-architecture (дата звернення:

26.11.2023).

9. FortiSASE. Concept Guide. Fortinet. URL: https://docs.fortinet.com/document/fortisase/latest/concept-guide/891466/introduction (дата звернення: 26.11.2023).

10. FortiSASE. Architecture Guide. Fortinet. URL: https://docs.fortinet.com/document/fortisase/latest/architecture-guide/308001/design-topology (дата звернення: 26.11.2023).

11. FortiSASE. Administration Guide. Fortinet. URL: https://docs.fortinet.com/document/fortisase/latest/administration-guide/756835/introduction (дата звернення: 26.11.2023).

12. Ворона О. А. Технологія забезпечення безпечної роботи гібридних працівників організації на базі FortiSASE. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 27 жовтня 2023. Тези доповідей. С. 58-60. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf (дата звернення: 26.11.2023).