ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ МАЛОГО АБО СЕРЕДНЬОГО БІЗНЕСУ НА БАЗІ MICROSOFT 365 BUSINESS PREMIUM»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Корж В. І.
(прізвище та ініціали)
Керівник Собчук А. В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ABSTRACT

Master’s thesis: 59 pages, 12 figures, 13 sources.

Object of research – the user access control to the organization's virtual machines when using cloud platforms.

Subject of research – the technology of user access control to the organization's virtual machines in Azure.

The aim of research – to develop the procedure for applying user access management technology to the organization's virtual machines when using cloud platforms and recommendations for its implementation.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison.

Businesses are increasingly experiencing increasingly sophisticated cyberattacks. To ensure security and business continuity, comprehensive automated protection solutions are used to quickly detect and respond to threats. One such end-to-end solution is Microsoft 365 Business Premium.

The paper analyzes the problem of protecting information resources for small and medium-sized businesses, defines its goals and objectives. The analysis of existing technologies for protecting information resources for small and medium-sized businesses was carried out. The methods and means of protecting information resources of the Microsoft 365 Business Premium solution are investigated. The purpose, main functions and composition of the means of protecting information resources of the Microsoft 365 Business Premium solution are determined.

Based on the research conducted in the work, the procedure for applying the technology for protecting information resources of the Microsoft 365 Business Premium solution is proposed. Recommendations have been developed for cybersecurity specialists on the use of information resource protection technology for small and medium-sized businesses.

Field of use – cybersecurity of corporate information system.

INFORMATION SYSTEM OF ORGANIZATION, INFORMATION RESOURCES, PROTECTION OF INFORMATION RESOURCES, TECHNOLOGY OF PROTECTION OF INFORMATION RESOURCES

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

AWS – Amazon Web Services

BGP – Border Gateway Protocol

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

OWASP – Open Web Application Security Project

RDP – Remote Desktop Protocol

SMB – Small and Medium-sized Businesses

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Підприємства все частіше зазнають дедалі складніших кібератак. В епоху технологій і гібридної роботи зростають ризики для малого й середнього бізнесу, оскільки таким клієнтам бракує коштів та спеціалізованої допомоги в питаннях безпеки.

Атаки зловмисних програм із вимогою викупу становлять найбільшу небезпеку для малого бізнесу. Більш ніж половина загальної кількості жертв – саме невеликі компанії. Фахівці відмічають, що за минулий рік кількість атак зловмисних програм із вимогою викупу зросла в кілька разів. За минулий рік чверть малих і середніх компаній зазнали порушення вимог безпеки. За оцінками фахівців, середні збитки підприємств від одного порушення безпеки даних становлять 108 тисяч доларів США.

Для забезпечення безпеки та безперебійної роботи застосовують комплексні рішення для автоматизованого захисту, щоб швидко виявляти загрози й реагувати на них. Одним із таких комплексних рішень є Microsoft 365 Business Premium.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології захисту інформаційних ресурсів на прикладі рішення Microsoft 365 Business Premium.

Об'єкт дослідження – захист інформаційних ресурсів для малого або середнього бізнесу.

Предмет дослідження – технологія захисту інформаційних ресурсів для малого або середнього бізнесу на прикладі Microsoft 365 Business Premium.

Мета роботи – розробити порядок застосування технології захисту інформаційних ресурсів для малого або середнього бізнесу та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту інформаційних ресурсів для малого або середнього бізнесу;

проаналізувати підходи до захисту інформаційних ресурсів для малого або середнього бізнесу;

проаналізувати існуючі рішення із захисту інформаційних ресурсів для малого або середнього бізнесу;

проаналізувати методи та засоби захисту інформаційних ресурсів для малого або середнього бізнесу на прикладі Microsoft 365 Business Premium;

розкрити порядок реалізації технології захисту інформаційних ресурсів для малого та середнього бізнесу.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту інформаційних ресурсів для малого або середнього бізнесу, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ [13].

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

1.1. Дослідження проблеми захисту інформаційних ресурсів для малого та середнього бізнесу

Малий і середній бізнес дуже часто не в змозі ефективно протидіяти кібератакам, оскільки таким клієнтам бракує ресурсів, коштів або спеціалізованої допомоги. Утім, вони потребують таких самих надійних технологій захисту, як і великі організації.

Порушення кібербезпеки є поширеним явищем в бізнесі. Зростаюча залежність від цифрових технологій означає, що малому бізнесу потрібна допомога з кібербезпеки. Загалом більше двох із п’яти (42%) підприємців кажуть, що вже стикалися з порушенням кібербезпеки. Три найпоширеніші загрози походять від зловмисного програмного забезпечення, фішингу та витоку даних (рис. 1.1) [11].

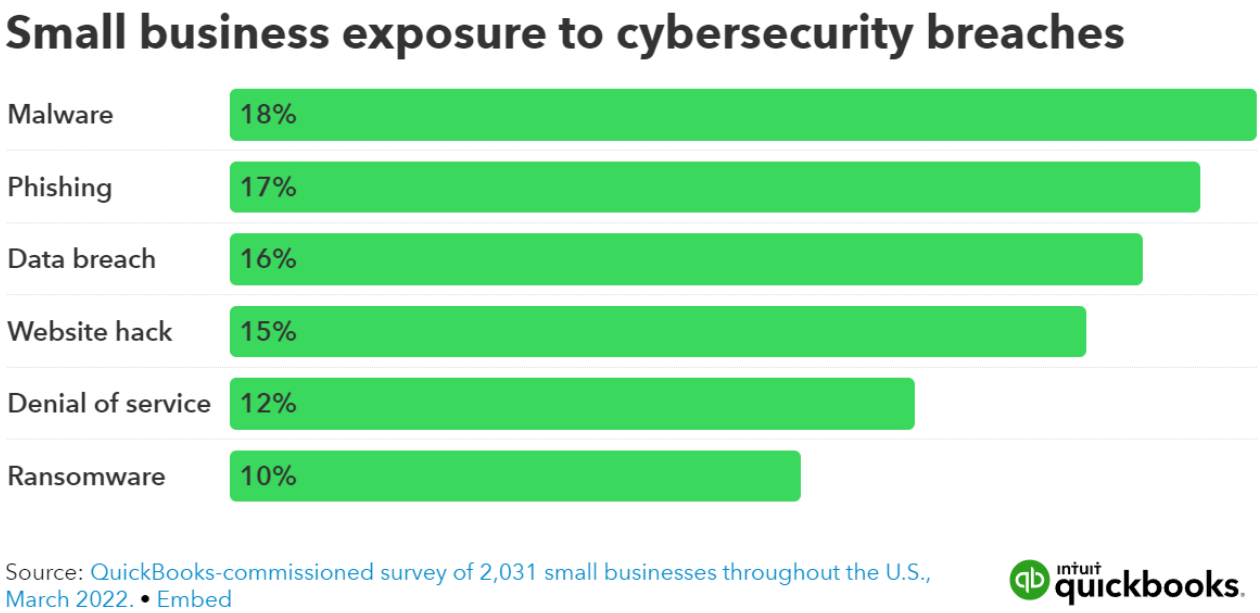

Рис. 1.1. Найпоширеніші загрози малому бізнесу [11]

Фактично, більше ніж кожен п’ятий малий бізнес (23%) описує кібербезпеку як одну з найбільших загроз, з якою вони зараз стикаються, випереджаючи низький попит і трохи відстаючи від грошових потоків [11].

Фахівці відмічають, що ландшафт кіберзагроз стрімко зростає та розвивається з року в рік. У таких умовах малий та середній бізнес (small and medium-sized businesses, SMB) стає все більшою мішенню. Насправді більше половини малих і середніх підприємств зазнали кібератак протягом останнього року [1].

У сучасному ландшафті кіберзагроз будь-яка компанія може стати об’єктом кібератаки. Через це малим і середнім підприємствам надзвичайно важко зосередитися на найважливішому – підтримувати свій бізнес рентабельним. Пересічний SMB просто не створений для того, щоб протистояти кібератаці, і, ймовірно, йому буде важко відновитися після втрат у випадку успішної кібератаки [1].

Малий і середній бізнес можна атакувати різними способами, але деякі ризики для кібербезпеки є більшими, ніж інші. Деякі з найбільших кіберзагроз, з якими стикаються SMB, це фішинг, втрата пароля та програмне забезпечення-вимагач [1].

Microsoft [3] визначає наступні основні загрози безпеки для даних, облікових записів та пристроїв:

шкідливе програмне забезпечення – це програмне забезпечення, яке може пошкодити комп'ютери або мережу і, можливо, викрасти дані, включаючи особисту інформацію або інформацію про клієнтів;

спам – це електронна пошта, яка не потрібна і може завалити поштову скриньку;

вірус – це шкідливе програмне забезпечення, яке націлене на вразливість у комп'ютерній системі підприємства та використовує Інтернет для поширення на інші системи;

фішинг та спуфінг – фішингові електронні листи виглядають так, ніби вони надіслані законною компанією або кимось, кого ви знаєте. Наприклад,

електронний лист, який видається відправленим із державної установи, може вимагати особисту інформацію, таку як пароль або номер рахунку. Фішингові електронні листи можуть містити «підроблену» електронну адресу. Наприклад, ви знаєте alice@contoso.com, але коли ви перевіряєте адресу електронної пошти, ваше повідомлення надходить від user@contoso1234c.com.

Уособлення також є формою фішингу: ваша електронна пошта походить від домену або користувача, дуже схожого на того, кого ви знаєте. Наприклад, повідомлення електронної пошти з адреси user@contosot.com на перший погляд виглядає так, ніби воно надійшло з адреси user@contoso.com;

шкідливі сайти чи файли – на шкідливих сайтах розміщуються віруси та шкідливе ПЗ. Бізнес може опинитися під загрозою, якщо працівник натисне на посилання, яке веде на шкідливий сайт. Посилання на шкідливі сайти часто надсилаються електронною поштою та включаються до повідомлень у соціальних мережах або реклами на веб-сайті. Кожен з них може включати уважну причину відвідування сайту.

Згідно зі звітом Verizon про розслідування витоку даних за 2021 рік, 46% зломів торкнулися малого та середнього бізнесу. У спільному звіті IBM та Ponemon Institute встановлено, що середня вартість витоку даних зросла на 10% у 2021 році, а дані Verizon свідчать про те, що вартість 95% інцидентів для малого та середнього бізнесу впала від 826 до 653 587 доларів США. Більше того, цим підприємствам часто бракує ресурсів для успішного захисту від атак [4].

Незалежно від своєї цілі, хакери зазвичай прагнуть отримати доступ до конфіденційних даних компанії, таких як інформація про кредитні картки споживачів. Маючи достатньо ідентифікаційної інформації, зловмисники можуть використати персональні дані особи будь-якою кількістю шкідливих способів.

Один із найкращих способів підготуватися до атаки – це зрозуміти різні методи, які зазвичай використовують хакери, щоб отримати доступ до цієї інформації. Хоча це аж ніяк не вичерпний перелік потенційних загроз, оскільки кіберзлочинність є явищем, що постійно розвивається.

Розширена постійна загроза або APT – це довгострокова цілеспрямована

атака, під час якої зловмисник зламує мережу в кілька етапів, щоб уникнути виявлення. Як тільки зловмисник отримує доступ до цільової мережі, він намагається залишатися непоміченим, закріплюючись у системі. Якщо порушення буде виявлено та усунено, зловмисник, можливо, вже знайшов інші маршрути в систему, щоб він міг продовжувати викрадення даних.

DDoS: розподілена атака типу «відмова в обслуговуванні» виникає, коли сервер навмисно перевантажується запитами, доки він не вимкне веб-сайт або мережеву систему цільового сервера.

Внутрішня атака: внутрішня атака виникає, коли хтось із правами адміністратора, як правило, всередині організації, навмисно зловживає своїми обліковими даними, щоб отримати доступ до конфіденційної інформації компанії. Колишні працівники, зокрема, становлять загрозу, особливо якщо вони залишили компанію на поганих умовах. У компанії має бути встановлений протокол для негайного скасування доступу до даних компанії після звільнення працівника.

Зловмисне програмне забезпечення: цей загальний термін є скороченням від «зловмисного програмного забезпечення» й охоплює будь-яку програму, запроваджену на комп’ютер цільової програми з метою завдати шкоди або отримати несанкціонований доступ. Типи зловмисного програмного забезпечення включають віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Знати це важливо, оскільки це допоможе визначити тип програмного забезпечення для кібербезпеки.

Атака «людина посередині» (MitM): у будь-якій звичайній транзакції дві сторони обмінюються товарами – або, у випадку електронної комерції, цифровою інформацією – одна з одною. Знаючи це, хакер, який використовує метод вторгнення MitM, робить це, встановлюючи шкідливе програмне забезпечення, яке перериває потік інформації, щоб викрасти важливі дані. Зазвичай це робиться, коли одна або кілька сторін проводять транзакцію через незахищену загальнодоступну мережу Wi-Fi, де хакер встановив зловмисне програмне забезпечення, яке просуває дані.

Атака на пароль. Існує три основні типи атак на пароль: атака методом

грубої сили, яка включає вгадування паролів, доки хакер не проникне в систему; атака за словником, яка використовує програму для спробування різних комбінацій словникових слів; і клавіатурний журнал, який відстежує натискання клавіш користувача, включаючи ідентифікатори входу та паролі.

Фішинг: можливо, це найпоширеніша форма кіберкрадіжки. Фішингові атаки включають збір конфіденційної інформації, як-от облікових даних для входу та даних кредитної картки, через веб-сайт, який виглядає легітимним (але зрештою шахрайським), який часто надсилається електронною поштою нічого не підозрюючим особам. Фішинг, розширена форма цього типу атак, вимагає глибоких знань про конкретних осіб і соціальної інженерії, щоб завоювати їх довіру та проникнути в мережу.

Програми- вимагачі: атака програм-вимагачів заражає комп'ютер жертви шкідливим програмним забезпеченням і, як випливає з назви, вимагає викуп. Як правило, програмне забезпечення-вимагач блокує ваш комп'ютер і вимагає гроші в обмін на відновлення доступу, або погрожує опублікувати особисту інформацію, якщо ви не заплатите вказану суму. Програмне забезпечення-вимагач є одним із найшвидше зростаючих типів порушень безпеки.

Атака SQL-ін'єкцій: більше чотирьох десятиліть веб-розробники використовували мову структурованих запитів (SQL) як одну з основних мов кодування в Інтернеті. Хоча стандартизована мова значно сприяла розвитку Інтернету, вона також може бути простим способом для шкідливого коду потрапити на веб-сайт підприємства. Завдяки успішній SQL-атаці на сервери зловмисники можуть отримувати доступ до важливих баз даних і змінювати їх, завантажувати файли та навіть маніпулювати пристроями в мережі.

Атака нульового дня: атаки нульового дня можуть стати найгіршою проблемою розробника. Це невідомі недоліки та експлойти в програмному забезпеченні та системах, виявлені зловмисниками до того, як розробники та співробітники служби безпеки дізнаються про будь-які загрози. Ці експлойти можуть залишатися невиявленими протягом місяців або навіть років, поки їх не виявлять і не виправлять.

1.2. Аналіз підходів до захисту інформаційних ресурсів для малого та середнього бізнесу

Оскільки все більше компаній розвивають свій бізнес в Інтернеті, потреба в надійних заходах кібербезпеки зростає паралельно. За даними Cybersecurity Ventures '2022 Cybersecurity Almanac, світові витрати на такі продукти зростуть до 1,75 трильйона доларів США за період з 2021 по 2025 роки, порівняно з 1 трлн доларів США за 2017-2021 роки [4].

Малі підприємства, які хочуть забезпечити свої мережі принаймні шансами протистояти багатьом атакам, повинні бути готові встановити базове програмне забезпечення безпеки [4].

Антивірусні рішення є найпоширенішими та захищають від більшості типів шкідливих програм. Апаратний або програмний брандмауер може забезпечити додатковий рівень захисту, запобігаючи неавторизованому доступу користувача до комп’ютера чи мережі. Більшість сучасних операційних систем, включаючи Windows 10 і 11, мають вбудований брандмауер [4].

Фахівці пропонують компаніям інвестувати в три додаткові засоби безпеки разом із інструментами поверхневого рівня [4], які розглянуто нижче.

Рішення для резервного копіювання даних: це гарантує, що інформацію, скомпрометовану або втрачену під час злому, можна легко відновити з альтернативного місця.

Програмне забезпечення для шифрування: щоб захистити конфіденційні дані, наприклад записи про співробітників, інформацію про клієнтів/клієнтів і фінансові звіти, компаніям слід розглянути можливість використання програмного забезпечення для шифрування.

Програмне забезпечення для двоетапної автентифікації або захисту паролем: використовуються ці інструменти з внутрішніми програмами, щоб зменшити ймовірність злому пароля.

Коли ви починаєте розглядати свої варіанти та заходи безпеки, які ви хотіли б застосувати, загалом доцільно провести оцінку ризику самостійно або за

допомогою сторонньої фірми.

Інвестуючи в рішення з кібербезпеки, малому та середньому бізнесу потрібно знайти оптимальний баланс доступних ресурсів, включаючи бюджет, вимоги, можливості та час. Крім того, вкрай важливо мати узгоджену стратегію кібербезпеки та план її виконання [10].

За останні кілька років кількість кібератак зросла як за частотою, так і за масштабом шкоди, яку вони можуть завдати. У середньому малий бізнес (10–49 співробітників) і середній бізнес (50–249 співробітників) несуть витрати, пов'язані з кібератаками, у розмірі прибл. $37 тис. і $68 тис. відповідно. Ця цитата з дослідження інформаційних ризиків Інституту Cyentia підкреслює вплив інциденту кібербезпеки на малий і середній бізнес: «Підприємство вартістю 100 мільярдів доларів США, яке зазнає типової кіберподії (292 тисячі доларів США), має очікувати витрати, які становлять 0,000003% річного доходу. З іншого боку, фірмовий магазин, який приносить 100 тисяч доларів на рік, швидше за все, втратить одну чверть своїх доходів (24 тисячі доларів) або більше» [10].

Повідомляється, що 71% малих і середніх підприємств мають лише базову оборонну інфраструктуру. Декілька проблем, з якими стикаються малого та середнього бізнесу під час покращення своєї позиції, включають бюджет, поведінку працівників, час і робочу силу. Через зростаючу загрозу безпеці малому та середньому бізнесу необхідно дотримуватися важливих практик кібербезпеки, формулюючи узгоджену стратегію кібербезпеки.

На основі Федеральної комісії зі зв'язку (Federal Communications Commission) та Forbes нижче наведено короткий виклад рекомендованих практик, які показано на рис. 1.2. Ці методи дозволять компаніям захистити свою IT-інфраструктуру та клієнтів від основних загроз кібербезпеці.

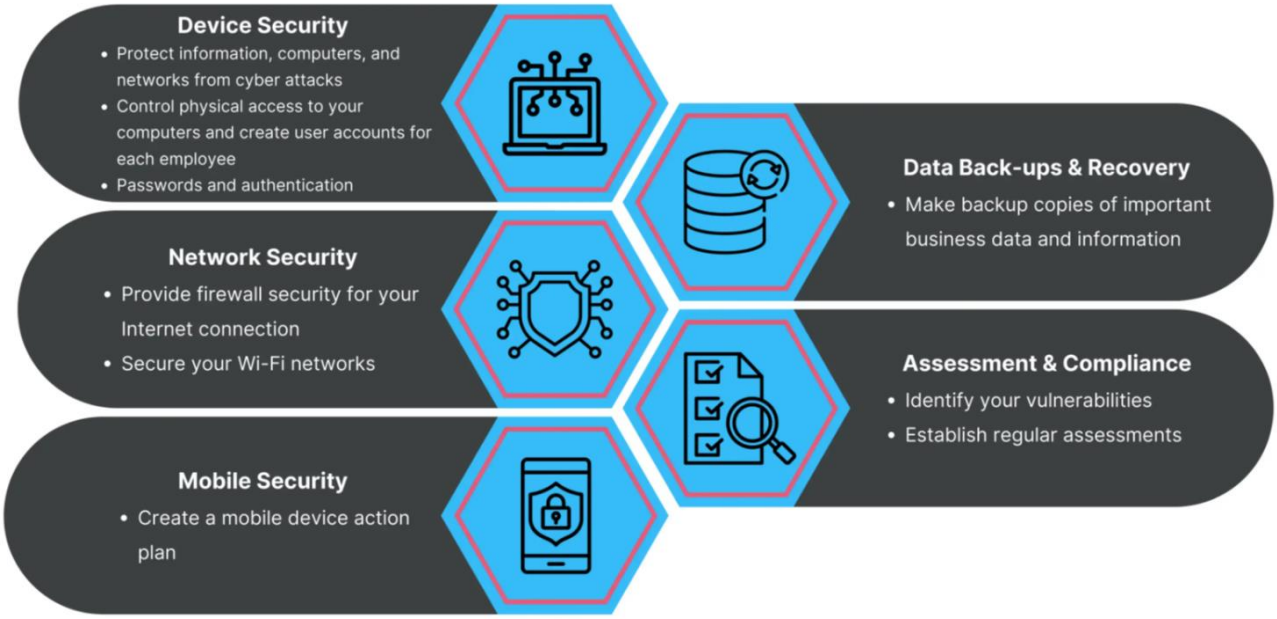

Рис. 1.2. Рекомендовані практики захисту інформаційних ресурсів малого та середнього бізнесу [10]

Продукти та рішення для кібербезпеки, які необхідні малому і середньому бізнесу показано на рисунку 1.3

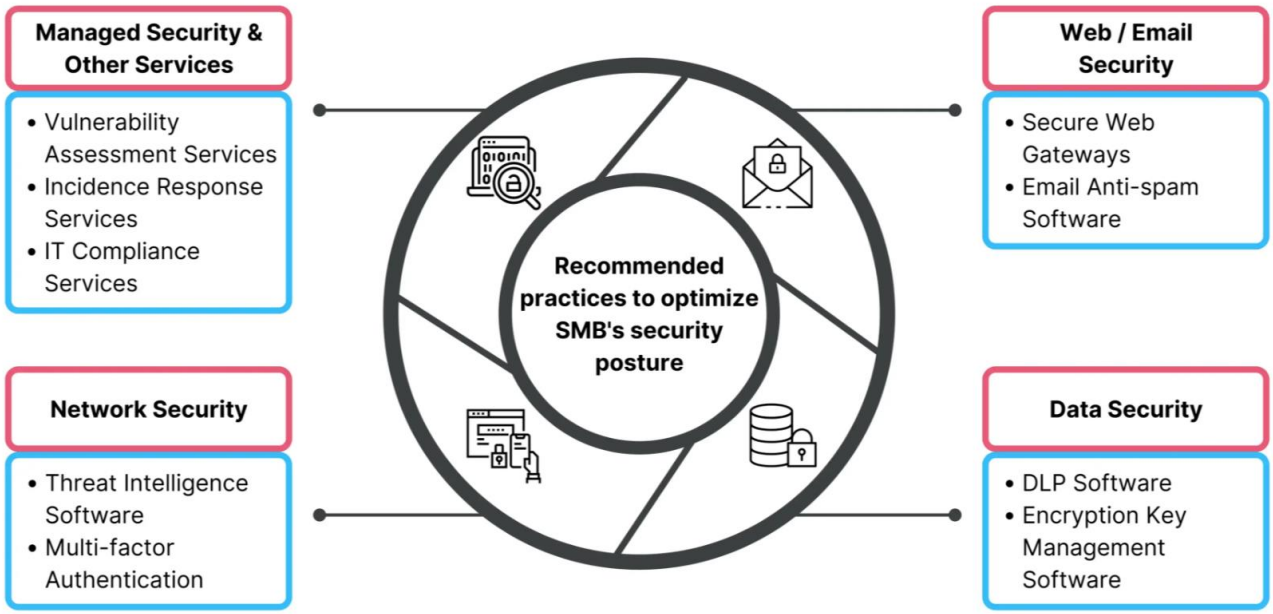

Рис. 1.3. Рекомендовані напрямки безпеки для SMB [10]

Вибрані продукти та рішення дозволять малим і середнім підприємствам

запровадити відповідні практики та оптимізувати їх стан кібербезпеки. Інші ключові сегменти включають керовану безпеку та інші послуги, а також безпеку додатків, зокрема такі продукти, як аналіз компонентів програмного забезпечення та програмне забезпечення безпеки контейнерів.

Очікується, що такі галузі, як системи та послуги охорони здоров'я, банківські та фінансові послуги, а також технології, медіа та телекомунікації, збільшать свої витрати на продукти/послуги кібербезпеки. Що стосується споживання, компанії вказали на збільшення витрат на такі сегменти продуктів, як мережева безпека, безпека кінцевих точок, ідентифікація та рішення для керування доступом [10].

Щоб побудувати або покращити стан кібербезпеки, малим і середнім підприємствам слід розглядати актуальні для бізнесу практики кібербезпеки та впровадити рішення з кібербезпеки з оптимальною окупністю інвестицій. Хоча продуктів/послуг може бути багато, компаніям традиційно доводиться орієнтуватися у величезному, часто заплутаному та керованому експертами ландшафті. Ринки кібербезпеки, налаштовані на потреби малого та середнього бізнесу, пропонують спеціалізовані функції як малому, середньому бізнесу, так і постачальникам, що робить їхню кібербезпеку та продажі ефективнішими.

1.3. Аналіз існуючих рішень із захисту інформаційних ресурсів для малого або середнього бізнесу

Малим підприємствам часто доводиться економно працювати, щоб зберегти прибуток і капітал, необхідний для розширення та коригування. Однак іноді це призводить до жертвування надійними системами безпеки заради безкоштовних пропозицій, які можуть не повністю відповідати їхнім потребам. У деяких випадках інструменти кібербезпеки, які використовують малі підприємства, ті самі, що розроблені для окремих користувачів.

Незалежно від розміру бізнесу, можна отримати інструменти, необхідні для захисту цифрових активів підприємства. Для забезпезпечення кібербезпеки для

малого бізнесу необхідно використовувати конкретні інструменти, які можна використовувати для посилення захисту від хакерів і взломів. Розглянемо ці питання більш детальніше.

Розширення можливостей малого та середнього бізнесу за допомогою технологій.

Існує багато типів рішень кібербезпеки для малого та середнього бізнесу, і отримання відповідного типу апаратного чи програмного забезпечення безпеки може дати бізнесу змогу максимізувати свій потенціал без шкоди для безпеки. Головне – вибрати технологію, яка дозволить вам бути на крок попереду зловмисників і різноманітної суміші загроз на ландшафті. Незалежно від того, чи хочете ви захистити співробітників, які використовують електронну пошту, ваші бізнес-додатки, веб-сайти чи кінцеві точки, є кілька варіантів на вибір [9].

Основні інструменти кібербезпеки для малого та середнього бізнесу.

Інструменти кібербезпеки, які ви виберете, залежатимуть від архітектури мережі підприємства. Але незалежно від того, як налаштована ваша цифрова інфраструктура, у вас є багато варіантів її захисту. Перший крок – визначити найцінніші цифрові активи, а також те, де ваша мережа може бути найбільш вразливою.

Для багатьох сучасних компаній найбільш явні вразливості знаходяться в кінцевих точках, які підключаються до їхньої мережі, на відміну від внутрішніх активів мережі. Витративши деякий час на аналіз того, хто і що підключається до мережі та як через неї проходять дані, полегшить максимальний захист. Розглянемо деякі інструменти, які можна використовувати для захисту бізнесу від програм-вимагачів, фішингу , хакерів та інших видів загроз.

Виявлення кінцевої точки та відповідь (Endpoint Detection and Response, EDR)

Рішення для виявлення та реагування на кінцеві точки (EDR) дозволяють легко виявляти пристрої, які підключаються до вашої мережі, і реагувати на загрози, які розпізнає система. Наприклад, якщо хтось підключається до вашої мережі та має зловмисні наміри, ваша система виявлення кінцевої точки та

відповіді може надати детальну інформацію про пристрій, який підключився, а також дані про його активність під час приєднання до вашої мережі. Окрім запобігання небажаним користувачам і пристроям від приєднання до вашої мережі, інструмент EDR також є потужним інструментом для збору криміналістичної інформації після витоку даних. Ви можете проаналізувати журнали, створені системою, щоб побачити, хто підключився, і визначити, чи вони відповідальні за порушення.

Антивірусне програмне забезпечення

Хоча антивірусне програмне забезпечення традиційно дуже добре бореться з комп'ютерними вірусами, сучасні антивірусні рішення також чудово справляються із захистом від інших видів загроз. Надійна антивірусна програма може виловлювати різноманітні атаки зловмисного програмного забезпечення , перевіряючи ваш комп'ютер на наявність відомих загроз.

Антивірусне програмне забезпечення використовує наявні профілі атак, які вплинули на користувачів. Він перевіряє вашу систему, щоб побачити, чи є на вашому комп'ютері такі шкідливі програми, інформує вас про небажані елементи та позбавляється від них. Отже, за допомогою правильного антивірусного програмного забезпечення ви можете захистити себе від багатьох найнебезпечніших загроз у кібернетичному середовищі.

Брандмауери наступного покоління (Next-Generation Firewalls, NGFW)

NGFW забезпечують широкий захист від цілої низки загроз, а також полегшують зовнішнім користувачам користуватися безпечними з'єднаннями з вашою мережею. Вони працюють, перевіряючи пакети даних, коли вони надсилаються до вашої мережі та з неї. Якщо виявлено відому загрозу, ваш NGFW може автоматично відхилити проблемний пакет даних.

Крім того, правильний тип брандмауера нового покоління використовує машинне навчання, яке може точно визначити зловмисну поведінку. Таким чином можна зупинити навіть атаки нульового дня , оскільки характер шкідливого коду можна виявити без попереднього інформування системи про його існування.

NGFW також можна використовувати для налаштування віртуальної

приватної мережі (virtual private network, VPN).

Захист системи доменних імен (Domain Name System, DNS)

Захист системи доменних імен (DNS) забезпечує додатковий рівень захисту, запобігаючи доступу співробітників до небезпечних веб-сайтів. Ці системи також можуть відфільтрувати вміст, який не має проникнення у вашу мережу, а також вміст, до якого ваші користувачі не мають доступу.

Наприклад, якщо працівник зазвичай відвідує веб-сайт із відомими загрозами у свій приватний час, він може спробувати підключитися до того самого сайту під час роботи. Ваша служба захисту DNS може заборонити їм підключатися до неї, коли вони знаходяться у вашій мережі.

Безпека шлюзу електронної пошти

Завдяки безпеці шлюзу електронної пошти ви можете запобігти проникненню небажаної електронної пошти в облікові записи ваших користувачів. Це включає як неприємну електронну пошту, як-от спам, так і більш прямі загрози, як-от електронні листи зі зловмисним програмним забезпеченням.

Наприклад, припустімо, що у вас є ще один невеликий офіс, підключений до основної бази операцій через програмно визначену глобальну мережу (software-defined wide-area network, SD-WAN), і ви хочете переконатися, що всі користувачі захищені, незалежно від того, де вони знаходяться. Завдяки системі безпеки шлюзу електронної пошти, поки вони користуються службою електронної пошти вашого малого бізнесу, вони не отримуватимуть ті повідомлення, які ви вважаєте небезпечними чи небажаними. Це утримує загрози за межами вашої мережі, а також гарантує, що місце для зберігання електронної пошти не витрачається на спам.

Виявлення та запобігання вторгненням (Intrusion Detection and Prevention, IDS/IPS)

Системи виявлення та реагування на вторгнення перевіряють вміст пакетів даних, коли вони намагаються проникнути у вашу мережу. Це відрізняє його від традиційного брандмауера, який перевіряє інформацію всередині заголовків

пакетів даних.

За допомогою системи виявлення та запобігання вторгненням ви можете блокувати багато різних типів загроз, особливо якщо ваша система використовує комплексну платформу аналізу загроз для виявлення шкідливого коду.

Ведення журналів і моніторинг журналів

Реєстрація подій, які впливають на вашу мережеву та моніторингову діяльність, може полегшити зупинку загроз і з'ясувати, як вони проникли у вашу систему у разі зламу. Журнали містять детальну інформацію, включно з описом активності з мітками часу, що значно полегшує кореляцію атак із пристроями чи користувачами, які могли бути причиною.

Захист кінцевої точки

Захист кінцевих точок зосереджується на забезпеченні безпеки ноутбуків, настільних ПК і мобільних пристроїв, які підключаються до вашої мережі. Це особливо важливо, коли у вашу мережу входять віддалені працівники. Оскільки ви не знаєте, яким загрозам можуть піддаватися їхні пристрої, коли вони не підключені до вашої системи, важко захиститися від загроз, які вони можуть представляти.

За допомогою захисту кінцевих точок ви можете посилити захист кожного пристрою, який користувачі підключають до вашої мережі, ефективно розширюючи межі вашого внутрішнього захисту.

Служби автентифікації/VPN

За допомогою служби автентифікації ви можете запобігти проникненню небажаних користувачів і хакерів у вашу мережу. Це робиться шляхом опису системи керування привілейованим доступом (PAM), яка змушує користувачів автентифікувати свою особу перед підключенням до вашої системи.

Використання VPN – це простий спосіб запобігти потенційно небезпечним користувачам отримати доступ до ваших цифрових активів. Завдяки VPN ви можете не тільки вимагати від усіх користувачів надати облікові дані для входу, але також можете зашифрувати всі дані, якими обмінюються між ними та вашою системою. Таким чином їхні пристрої, а також ваша мережа захищені від

зовнішніх загроз.

Хмарна безпека

Хмарна безпека – це широкий термін, який стосується технологій і політик, які використовуються для захисту хмарних активів від кібератак. Такі рішення захищають хмарні ресурси, наприклад: дані, додатки, послуги, хмарна інфраструктура.

Брандмауери веб-додатків

Брандмауери веб-додатків (Web application firewalls, WAF) захищають ваші веб-додатки від хакерів, які можуть спробувати проникнути в них, щоб викрасти інформацію або використати вразливість у веб-додатку. Увесь трафік, що надсилається до вашої веб-служби та йде від неї, фільтрується, і якщо виявлено загрозу, пов’язані з нею дані можуть бути автоматично видалені.

Багато малих і середніх підприємств використовують WAF для захисту своїх веб-активів від хакерів, розподілених атак типу «відмова в обслуговуванні» (DDoS) та інших інтернет-загроз.

SD-WAN

Програмно визначені глобальні мережі (SD-WAN) дають вам можливість контролювати спосіб управління трафіком із детальними деталями. Використовуючи SD-WAN, ви можете оптимізувати використання ваших цифрових ресурсів, забезпечуючи належну підтримку та водночас кібербезпеку. Замість того, щоб ваш трафік подорожував мережею випадковим чином, ви можете наказати певним видам даних відправлятися в одне місце, а інші – кудись інше. Це забезпечує більш стабільну та безпечну роботу для користувачів.

За допомогою SD-WAN ви також можете зменшити витрати, пов’язані з пропускною здатністю, оскільки ви отримуєте більше від поточної послуги.

Керування паролями підприємства/керування привілейованим доступом (Privileged Access Management, PAM)

Завдяки керуванню корпоративними паролями та PAM ви отримуєте контроль над діяльністю та ідентифікацією всіх користувачів і пристроїв, які підключаються до вашої мережі. Лише ті, хто отримав облікові дані доступу,

можуть взаємодіяти з вашою мережею, і якщо їхня діяльність стає проблематичною, ви можете відкликати їхні привілеї.

Крім того, якщо користувач більше не відповідає вимогам, наприклад, коли його було виключено з вашої компанії, ви можете легко переконатися, що він більше не зможе потрапити у вашу систему.

Управління вразливістю та загрозами

Управління вразливістю та загрозами включає в себе зменшення вразливості вашого бізнесу до загроз, а також забезпечення належного захисту кінцевих точок і стійкості вашої компанії у разі злому. Для цього потрібен систематичний підхід із залученням технологій, таких як засоби захисту кінцевих точок, політики та люди.

Оцінка вразливості також потребує системи звітування про проблеми, що дозволить вам усунути недоліки та запобігти серйозним порушенням у майбутньому.

Виявлення загроз

Виявлення загроз передбачає аналіз усіх активів, підключених до вашої мережі, а також самої мережі на предмет підозрілої активності, програм і користувачів. Система виявлення загроз використовує дані, згенеровані різними подіями у вашій мережі, щоб виявити проблеми з кібербезпекою. Це також може включати пісочницю , яка містить загрози в ізольованому середовищі, утримуючи їх подалі від чутливих зон вашої мережі. Поки загроза знаходиться в цьому контрольованому середовищі, її діяльність ретельно відстежується, що дозволяє адміністраторам вивчати її та вчитися на ній [9].

Так, Fortinet Security Fabric надає малим і середнім підприємствам комплексний захист від широкого спектру кіберзагроз, захищаючи їх мережу з кількох різних точок одночасно. Security Fabric гарантує [9]:

хмарні засоби безпеки;

захист пристроїв на межі вашої мережі;

захист кінцевих точок;

захист бізнес-користувачів.

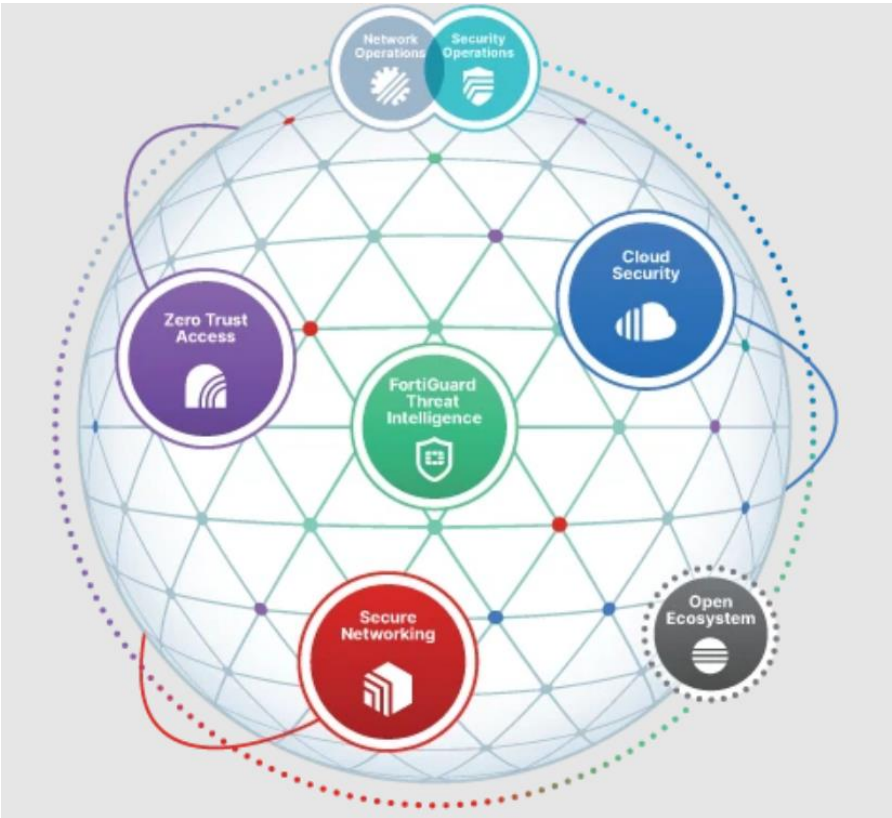

Рис. 1.4. Технології захисту Fortinet Security Fabric [9]

Fortinet Security Fabric (рис. 1.4) поєднує нульову довіру, хмарну безпеку з автоматичним масштабуванням і безпекову мережу, щоб небажані користувачі та трафік не заважали вашим бізнес-операціям.

Отже, інструменти, необхідні для кібербезпеки, включають виявлення та реагування на кінцеву точку (EDR), антивірусне програмне забезпечення, брандмауери нового покоління (NGFW), захист системи доменних імен (DNS), безпеку шлюзу електронної пошти, виявлення та запобігання вторгненням, ведення журналів і моніторинг журналів, захист кінцевих точок, служби автентифікації та віртуальна приватна мережа (VPN), хмарна безпека, брандмауери веб-додатків (WAF), програмно визначені глобальні мережі (SD-WAN), керування корпоративними паролями, керування привілейованим доступом (PAM), керування вразливістю та загрозами і виявлення загроз.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ РІШЕННЯ MICROSOFT 365 BUSINESS PREMIUM

2.1. Призначення та основні функції рішення Microsoft 365 Business Premium

Рішення Microsoft 365 Business Premium із інструментами підвищення продуктивності світового класу є розумним вибором для малого та середнього бізнесу. Розроблений з урахуванням кібербезпеки, рішення Microsoft 365 Business Premium пропонує захист інформаційних ресурсів організацій від хакерів і кібератак, включаючи випадкових осіб, організовану злочинність або високорозвинені національні держави [2].

Microsoft 365 Business Premium – це комплексне хмарне рішення для продуктивності й безпеки, розроблене та створене для малого та середнього бізнесу (до 300 співробітників). Рішення Microsoft 365 Business Premium забезпечує [2]:

можливість співробітникам бути на зв’язку та працювати продуктивно, незалежно від того, чи працюють вони на місці чи віддалено, за допомогою найкращих у своєму класі інструментів для співпраці, таких як Microsoft Teams;

можливість надання своїм співробітникам безпечного доступу до їхніх бізнес-даних і додатків і забезпечує лише авторизований доступ персоналу до конфіденційних робочих даних;

захист від складних кіберзагроз і захист своїх бізнес-даних за допомогою розширеного захисту від фішингу, програм-вимагачів і втрати даних;

керування та захист пристроїв (Windows, Mac, iOS та Android), які підключаються до даних, допомога у підтримуванні цих пристроїв в актуальному стані.

Microsoft 365 Business Premium – це комплексна послуга передплати для компаній із кількістю співробітників менше 300 осіб. Він інтегрує додатки та

служби Office для підвищення продуктивності та інструменти для співпраці, такі як Microsoft Teams, із розширеними можливостями безпеки та керування пристроями (рис. 2.1).

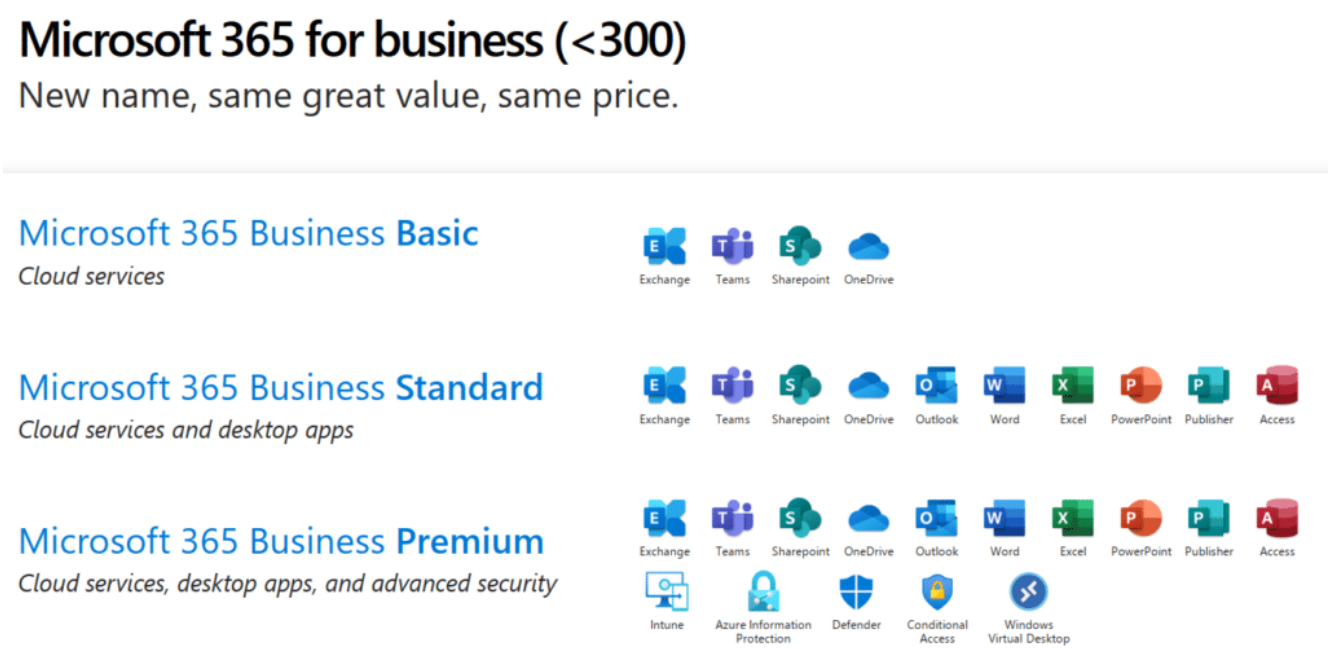

Рис. 2.1. Відмінності рішень Microsoft 365 Business Premium

Бізнес-дані можуть бути скомпрометовані різними способами. Користувачі можуть поставити під загрозу безпеку організації, коли здійснюється вхід в систему за допомогою скомпрометованих облікових даних або переглядаються дані організації на різних пристроях і додатках. Зокрема, якщо організація знаходиться під загрозою:

зламані або слабкі облікові дані для входу;

зламаний пристрій або пристрій, що належить користувачу;

користувачі, які можуть копіювати/вставляти/зберігати дані організації в особистих додатках;

користувачі, які встановлюють і використовують програми сторонніх розробників із слабким захистом;

вразливості електронної пошти, зокрема обмін конфіденційними даними, спроби фішингу, зловмисне програмне забезпечення тощо;

коли люди, які не мають право, можуть отримати доступ до документів із конфіденційною інформацією.

Рішення Microsoft 365 Business Premium допомагає захистити дані підприємства в кожному з цих випадків. Функції безпеки, які захищають бізнес-дані, показано на рис. 2.2.

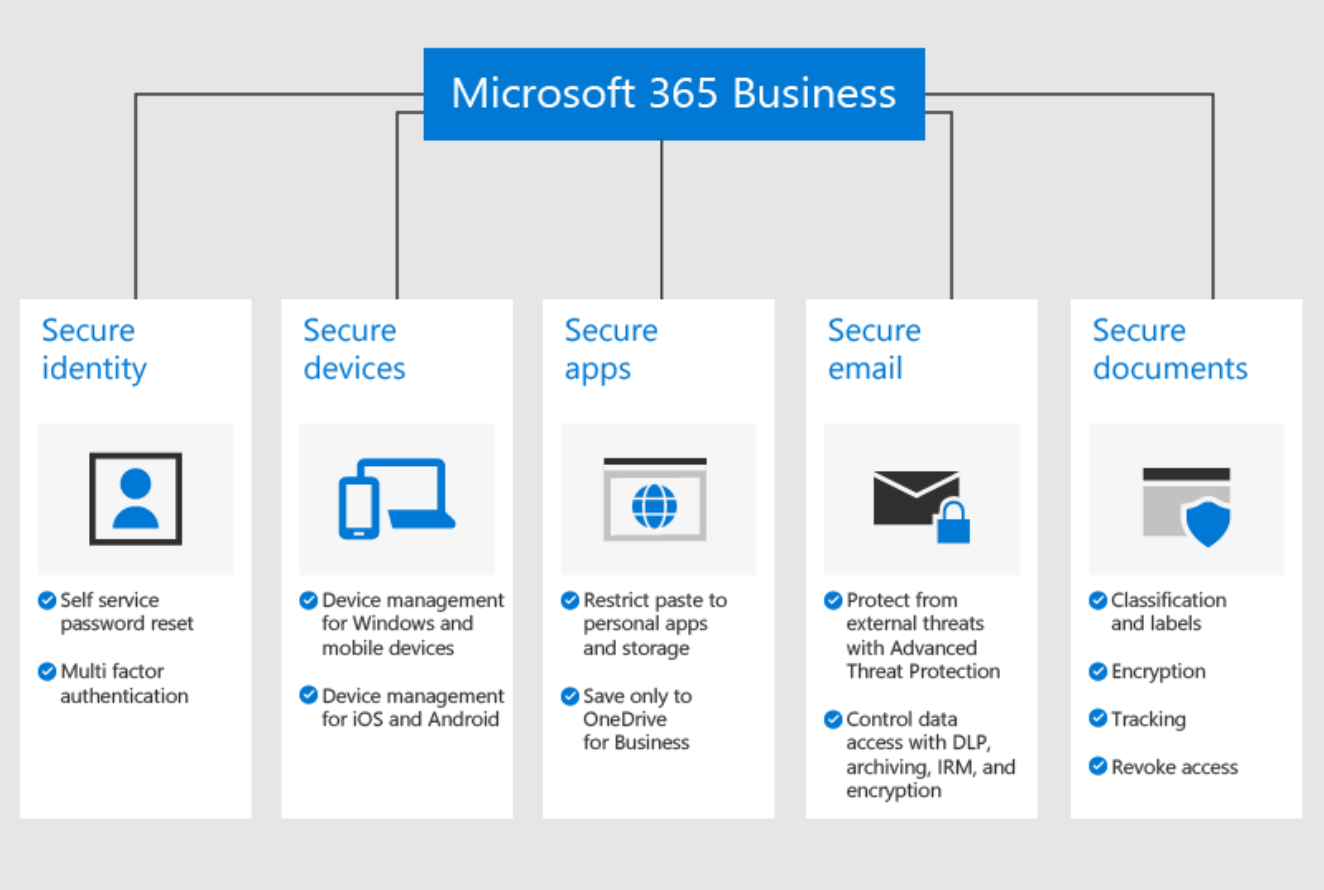

Рис. 2.2. Функції безпеки рішення Microsoft 365 Business Premium

Повнофункціональне рішення Microsoft 365 Business Premium для забезпечення захисту включає всі можливості Microsoft Defender for Business та переваги:

захист електронної пошти від фішингових атак за допомогою Microsoft Defender для Office 365;

захист робочих даних на особистих пристроях за допомогою Microsoft Intune;

безпечний доступ до робочих програм завдяки Azure AD Premium (план 1);

захист від утрати або крадіжки паролів завдяки засобам удосконаленої

багатофакторної автентифікації;

безпека інформації за допомогою засобу захисту від втрати даних і захисту даних в Azure;

архівування й витребування електронної інформації та судове утримання;

найкращі у своєму класі програми Office і потужні хмарні служби;

співпраця в чаті й на онлайн-нарадах у Microsoft Teams;

1 ТБ простору в хмарному сховищі для кожного користувача у OneDrive.

Рішення Microsoft 365 Business Premium реалізує наступні функції [2]:

управління правами користувачів; оцінка конфігурації;

сканування даних, що зберігаються в хмарі, за запитом;

запобігання втрати даних і виявлення загроз;

забезпечення відповідності, включаючи SOX, GDPR, PCI, HIPAA, NIST і ISO27001;

моніторинг поведінки та активності користувачів.

2.2. Призначення та основні функції рішення Microsoft Defender for Business

Простий комплексний захист кінцевих точок, який допоможе захистити ваш бізнес і зосередитися на важливому. Defender for Business доступний як окрема підписка та входить до складу Microsoft 365 Business Premium [7].

Defender for Business – це нове рішення для захисту кінцевих точок, розроблене спеціально для малого та середнього бізнесу (до 300 співробітників). За допомогою цього рішення безпеки кінцевих точок пристрої вашої компанії краще захищені від програм-вимагачів, шкідливих програм, фішингу та інших загроз.

Розглянемо компоненти рішення Defender for Business.

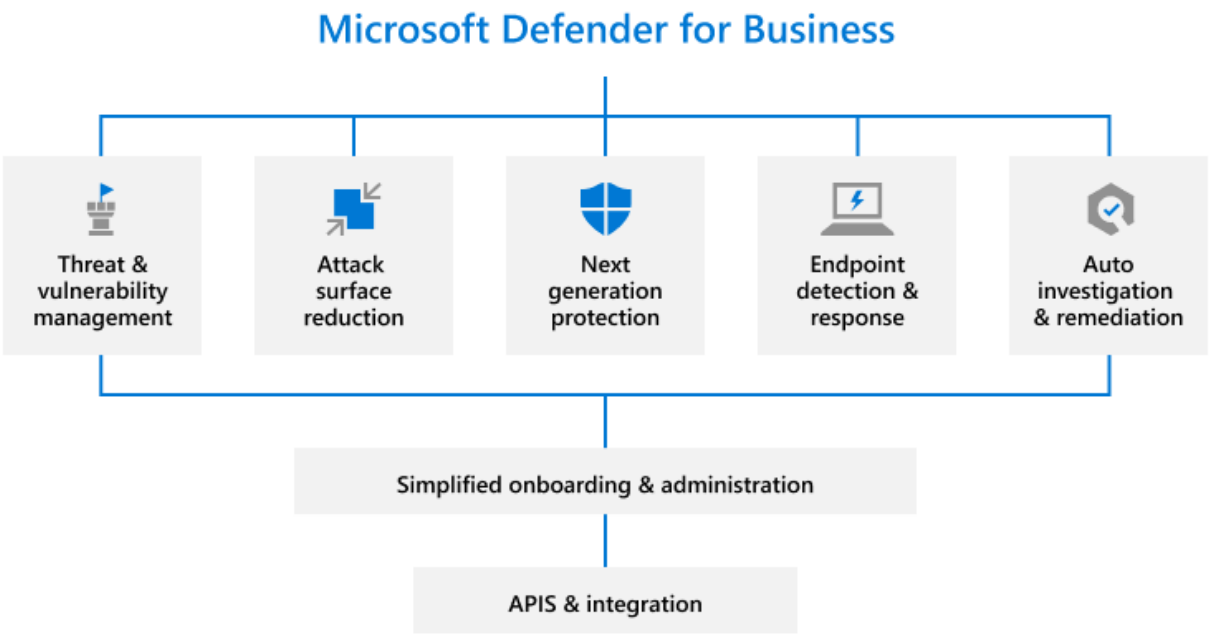

Рис. 2.3. Основні функції захисту рішення Microsoft Defender for Business [7]

За допомогою Defender for Business ви можете захистити пристрої та дані, які використовує ваш бізнес, за допомогою [4]:

безпека корпоративного рівня. Defender for Business пропонує потужні можливості захисту кінцевих точок від нашого провідного в галузі рішення Microsoft Defender for Endpoint і оптимізує ці можливості для IT-адміністраторів для підтримки малого та середнього бізнесу;

просте у використанні рішення безпеки. Defender for Business пропонує спрощений досвід, який направляє вас до дій за допомогою рекомендацій і аналізу безпеки ваших кінцевих точок. Спеціальні знання не потрібні, оскільки Defender for Business пропонує конфігурацію, керовану майстром, і стандартні політики безпеки, розроблені для захисту пристроїв вашої компанії з першого дня;

гнучкість для вашого середовища. Defender for Business може працювати з вашим бізнес-середовищем, незалежно від того, чи використовуєте ви Microsoft Intune, чи новачок у Microsoft Cloud. Defender for Business працює з компонентами, вбудованими в Windows, і з програмами для пристроїв Mac, iOS і Android;

інтеграція з Microsoft 365 Lighthouse, інструментами RMM і програмним забезпеченням PSA . Якщо ви є постачальником хмарних рішень (CSP) Microsoft і використовуєте Microsoft 365 Lighthouse, ви можете переглядати інциденти безпеки та сповіщення клієнтів ваших клієнтів (див. Microsoft 365 Lighthouse і Defender for Business). Якщо ви є постачальником керованих послуг Microsoft (MSP), ви можете інтегрувати Defender for Business зі своїми інструментами віддаленого моніторингу та керування (RMM) і програмним забезпеченням для автоматизації професійних послуг (PSA).

Microsoft Defender for Business має спрощений процес налаштування, розроблений спеціально для малого та середнього бізнесу. Досвід, схожий на майстра, позбавить вас від здогадок під час реєстрації та керування пристроями. Ми рекомендуємо використовувати спрощений процес конфігурації, але ви не обмежені цією опцією.

Щоб підключити пристрої та налаштувати параметри безпеки для пристроїв вашої компанії, ви можете вибрати один із наведених нижче способів:

спрощений процес налаштування в Microsoft Defender for Business;

використовуйте Microsoft Intune.

Спрощене налаштування на порталі Microsoft 365 Defender.

Спрощена конфігурація включає досвід, подібний до майстра, який допоможе вам налаштувати та налаштувати Defender for Business. Спрощена конфігурація також включає параметри безпеки за замовчуванням і політики, які допомагають захистити пристрої підприємства, щойно вони підключаються до Defender for Business. Ви можете переглядати та редагувати стандартні політики відповідно до потреб свого бізнесу.

Завдяки спрощеному досвіду ваша команда безпеки використовує портал Microsoft 365 Defender як єдине місце, щоб:

налаштувати та налаштувати Defender for Business;

перегляд інцидентів і керування ними;

реагувати на загрози та пом’якшувати їх;

переглянути звіти;

перегляд незавершених або завершених дій.

Центр адміністрування Microsoft Endpoint Manager

Microsoft Intune – це хмарний постачальник керування мобільними пристроями (MDM) і керування мобільними програмами (MAM) для програм і пристроїв. Якщо ви вже використовуєте Intune, ви можете продовжувати використовувати центр адміністрування Endpoint Manager для керування такими пристроями, як мобільні телефони, планшети та ноутбуки.

2.3. Зміст технології захисту інформаційних ресурсів в Microsoft 365 Business Premium

Розглянемо зміст технології захисту інформаційних ресурсів Microsoft 365 Business Premium, схема якої показано на рис. 2.4.

Перший етап – захист середовища інформаційних ресурсів організації. Ці дії виконує адміністратор системи. Він забезпечує базовий процес налаштування Microsoft 365 для організації, додає користувачів, призначає ліцензії та налаштовує свій домен для роботи з Microsoft 365. На цьому етапі підвищується рівень захисту, виконуються важливі заходи забезпечення безпеки на передовій лінії, щоб запобігти кібератакам. Налаштовується багатофакторна автентифікація (MFA), захищаються облікові записи адміністратора та забезпечується захист від зловмисного програмного забезпечення та інших загроз [2].

Рис. 2.4. Зміст технології захисту інформаційних ресурсів [2]

Адміністратор системи здійснює покроковий процес налаштування користуючись інструментами центру адміністрування Microsoft 365 (рис. 2.4, 2.5).

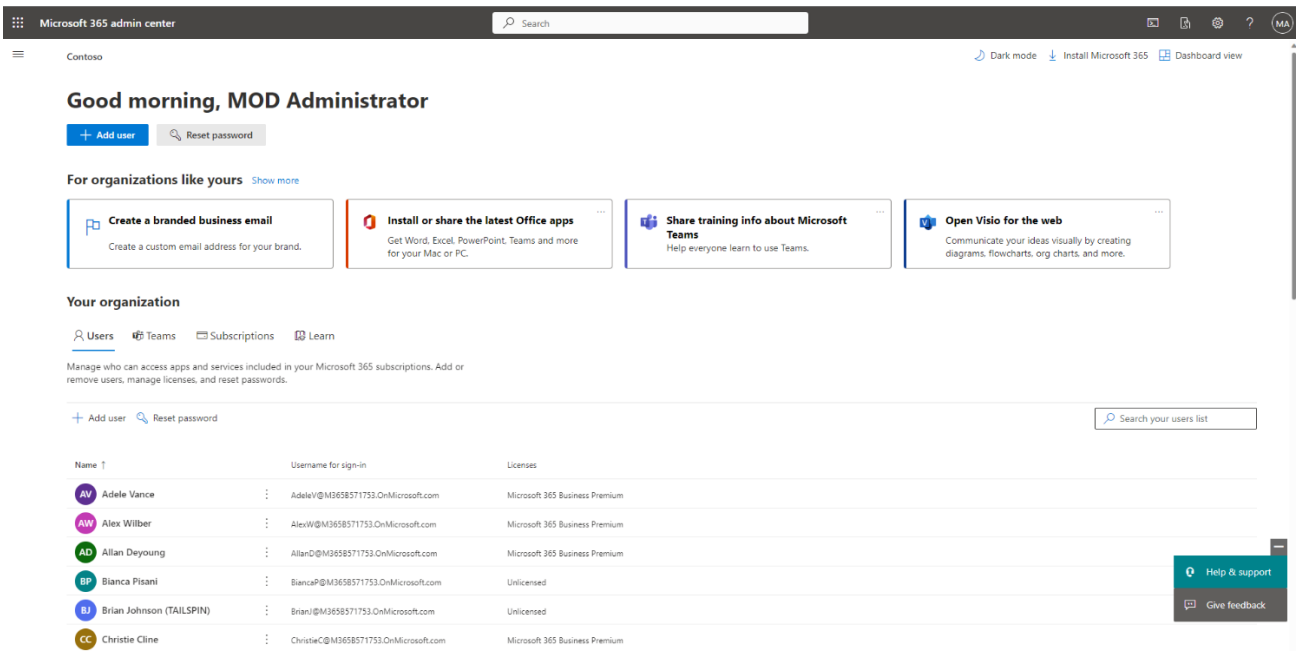

Рис. 2.4. Центр адміністрування Microsoft 365 [2]

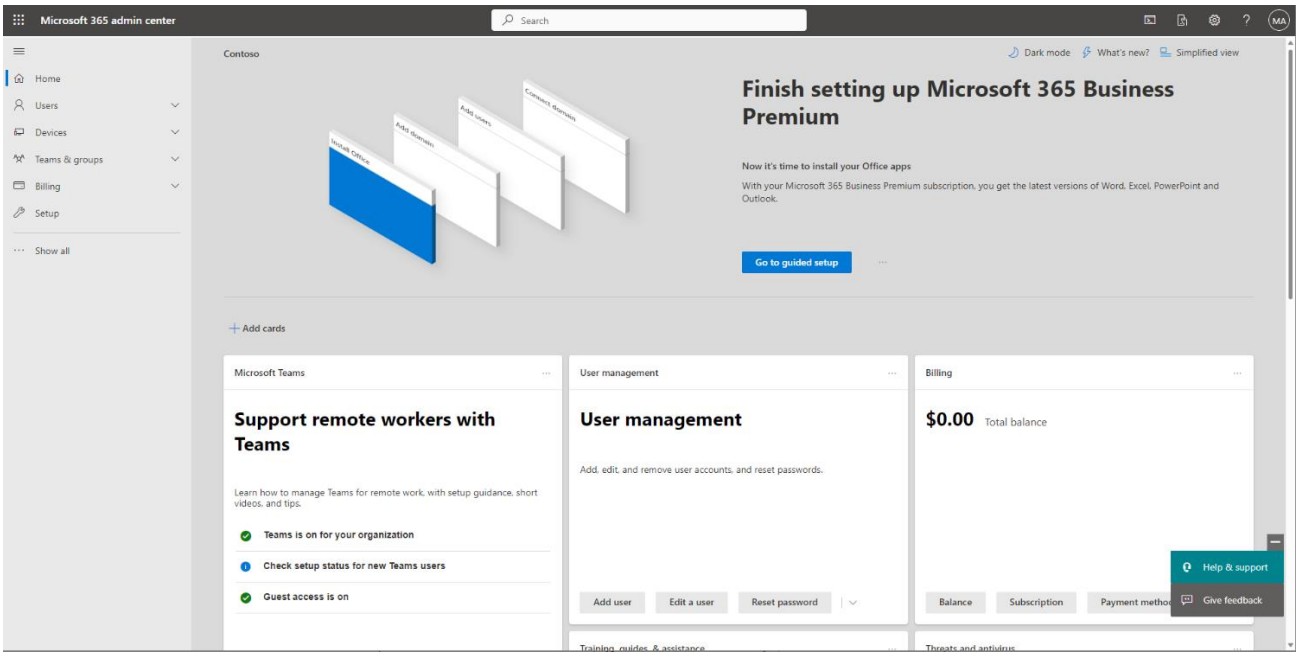

Рис. 2.5. Панель покрокового налаштування Microsoft 365 Business Premium [2]

Щоб додати користувача, адміністратор системи вводить його ім’я, прізвище та ім’я користувача, а потім натискає *Додати користувачів* і призначає

ліцензії. Крім того, адміністратор може вибрати *Переглянути всіх користувачів*, щоб перейти на сторінку активних користувачів, де він може переглядати, додавати та керувати користувачами (рис. 2.6).

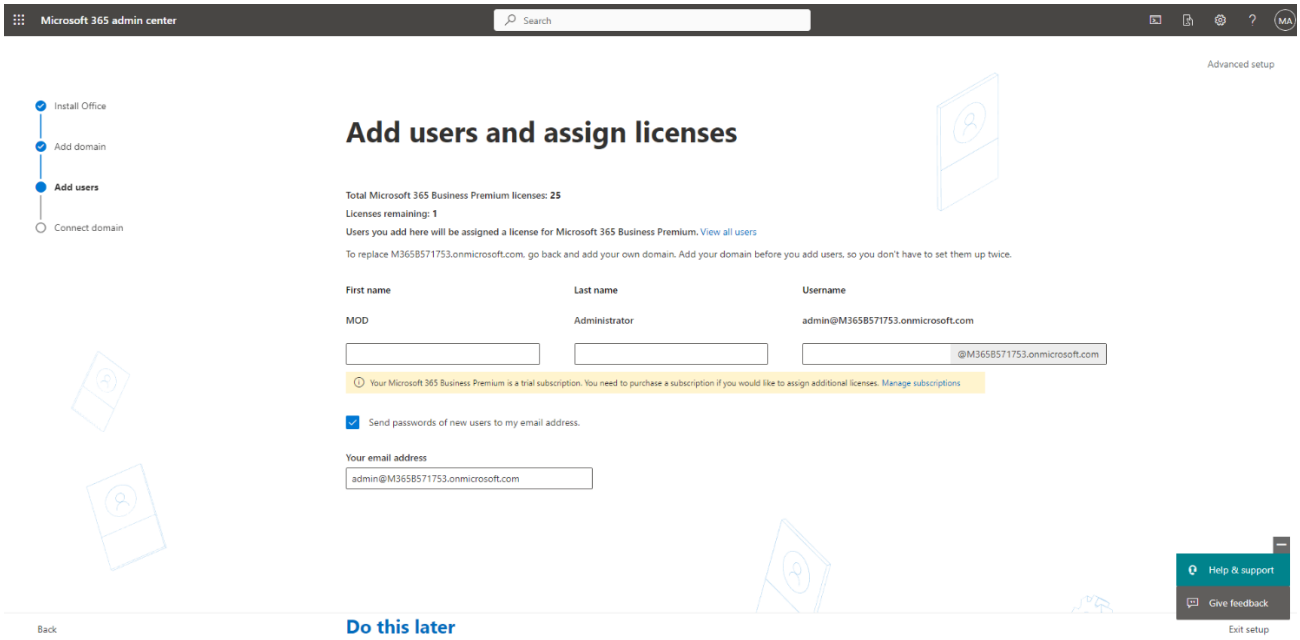

Рис. 2.6. Панель додання користувачів та призначення ліцензій [2]

Необхідно відмітити, що підприємства малого та середнього бізнесу визнають безпеку ключовим компонентом свого успіху, але часто не мають достатнього потенціалу чи досвіду, щоб мати спеціальну групу безпеки [2].

Це вирішується шляхом інтеграції захисту кінцевих точок Microsoft із інструментами RMM і програмним забезпеченням PSA. Підприємства – постачальники послуг, керованих корпорацією Microsoft (Microsoft Managed Service Provider, MSP), можуть інтегрувати захист кінцевих точок Microsoft із інструментами віддаленого моніторингу та керування (remote monitoring and management, RMM) і програмним забезпеченням для автоматизації професійних послуг (professional service automation, PSA) для того, щоб:

отримати доступ до порталу Microsoft 365 Defender своїх клієнтів, щоб усунути виявлені загрози та інциденти;

отримувати сповіщення електронною поштою про нові сповіщення або вразливі місця серед орендарів клієнтів;

збирати та переглядати інциденти та сповіщення за допомогою інструментів безпеки та керування подіями (SIEM);

організувати дії з усунення несправностей, як-от схвалення дій після автоматизованих розслідувань або виконання дій вручну на пристрої.

Інтеграцію можна здійснити за допомогою Defender for Endpoint APIs.

Виконуючи послідовність заходів можна посилити свій захист. Необхідно починаєте із застосування вимог багатофакторної автентифікації (MFA), використовуючи параметри безпеки за замовчуванням або умовний доступ. Ви налаштуєте різні ролі адміністратора та конкретні рівні безпеки для них. Доступ до облікових записів адміністратора є важливою метою для ворожих хакерів, і захист цих облікових записів є критично важливим, оскільки доступ і контроль, які вони надають, можуть вплинути на всю систему. Крім того, ви захистите вміст електронної пошти та пристрої. Для цього необхідно:

увімкнути параметри безпеки багатофакторної автентифікації за замовчуванням;

захистити облікові записи адміністратора;

захистити від шкідливих програм та інших загроз.

Після цих дій необхідно налаштувати некеровані пристрої (BYOD).

Стандартні налаштування безпеки та багатофакторна автентифікація.

Необхідно відмітити, що Microsoft 365 Business Premium розроблено, щоб захистити облікові записи користувачів компанії за допомогою попередньо налаштованих параметрів безпеки. Ці налаштування включають увімкнення багатофакторної автентифікації (MFA) для всіх корпоративних облікових записів адміністраторів і користувачів. Для більшості організацій параметри безпеки за умовчанням забезпечують хороший рівень безпеки входу. Для організацій, які повинні відповідати суворішим вимогам, можна використовувати умовний доступ.

Параметри безпеки за замовчуванням були розроблені, щоб допомогти захистити облікові записи користувачів компанії з самого початку. Якщо ввімкнено, параметри безпеки за замовчуванням забезпечують безпечні

параметри за замовчуванням, які допомагають захистити компанію за допомогою:

вимагання від усіх користувачів і адміністраторів зареєструватися в MFA за допомогою програми Microsoft Authenticator або будь-якої сторонньої програми за допомогою OATH TOTP.

виклику користувачам за допомогою MFA, здебільшого, коли вони з'являються на новому пристрої чи додатку, але частіше для критичних ролей і завдань;

вимкнення автентифікації застарілих клієнтів автентифікації, які не можуть виконувати MFA;

захисту адміністраторів, вимагаючи додаткової автентифікації кожного разу, коли вони входять до системи.

MFA – це важливий перший крок у захисті компанії, а стандартні налаштування безпеки спрощують увімкнення MFA. Якщо вашу підписку було створено 22 жовтня 2019 року або пізніше, параметри безпеки за замовчуванням могли бути автоматично ввімкнені для вас – вам слід перевірити свої налаштування, щоб підтвердити.

Якщо ви використовували параметри безпеки за замовчуванням, вам потрібно буде вимкнути їх перед використанням умовного доступу. Ви можете використовувати або параметри безпеки за замовчуванням, або політики умовного доступу, але ви не можете використовувати обидва одночасно.

Якщо компанія чи бізнес має складні вимоги до безпеки або вам потрібен більш детальний контроль над своїми політиками безпеки, вам слід розглянути можливість використання умовного доступу замість стандартних параметрів безпеки, щоб досягти подібного або вищого рівня безпеки.

Умовний доступ дає змогу створювати та визначати політики, які реагують на події входу та запитують додаткові дії, перш ніж користувачеві буде надано доступ до програми чи служби. Політики умовного доступу можуть бути детальними та конкретними, що дозволяє користувачам працювати продуктивно будь-де та будь-коли, а також захищає вашу організацію.

Параметри безпеки за замовчуванням доступні для всіх клієнтів, тоді як для

умовного доступу потрібен один із таких планів:

Azure Active Directory Premium P1 або P2;

Microsoft 365 Business Premium;

Microsoft 365 E3 або E5;

корпоративна мобільність і безпека E3 або E5.

Захистіть облікові записи адміністратора в Microsoft 365 Business Premium

Використовуйте облікові записи адміністратора лише для адміністрування Microsoft 365. Адміністратори повинні мати окремий обліковий запис користувача для регулярного використання програм Microsoft 365 і використовувати свій обліковий запис адміністратора лише тоді, коли це необхідно для керування обліковими записами та пристроями, а також під час роботи над іншими функціями адміністратора. Також доцільно видалити ліцензію Microsoft 365 зі своїх облікових записів адміністратора, щоб вам не довелося платити за додаткові ліцензії.

Якщо потрібно налаштувати принаймні ще один обліковий запис глобального адміністратора, щоб надати адміністративний доступ іншому довіреному співробітнику, тв ви можете створити окремі облікові записи адміністратора для керування користувачами (ця роль називається адміністратором керування користувачами).

Рекомендується налаштувати набір облікових записів адміністратора для обмеження кількості глобальних адміністраторів для організації. Крім того, рекомендується дотримуватися концепції доступу з найменшими привілеями, що означає, що ви надаєте доступ лише до даних і операцій, необхідних для виконання своїх завдань. Щоб захистити всі свої облікові записи адміністраторів, дотримуйтесь цих рекомендацій:

вимагайте від усіх облікових записів адміністратора використання автентифікації без пароля (наприклад, Windows Hello або програми автентифікації) або MFA;

уникайте використання спеціальних дозволів для адміністраторів. Замість того, щоб надавати дозволи певним користувачам, призначайте дозволи через

ролі в Azure Active Directory (Azure AD). І надайте доступ лише до даних і операцій, необхідних для виконання поставленого завдання;

використовуйте вбудовані ролі для призначення дозволів, де це можливо. Керування доступом на основі ролей (role-based access control, RBAC) Azure має кілька вбудованих ролей, якими можна користуватися.

Захистіть себе від шкідливих програм та інших кіберзагроз за допомогою Microsoft 365 Business Premium

Для цього необхідно переглянути та застосувати попередньо встановлені політики безпеки (рис. 2.7).

Підписка включає попередньо встановлені політики безпеки, які використовують рекомендовані налаштування для захисту від спаму, шкідливого програмного забезпечення та фішингу. За замовчуванням вбудований захист увімкнено. Однак розгляньте можливість застосування стандартного або суворого захисту для підвищення безпеки.

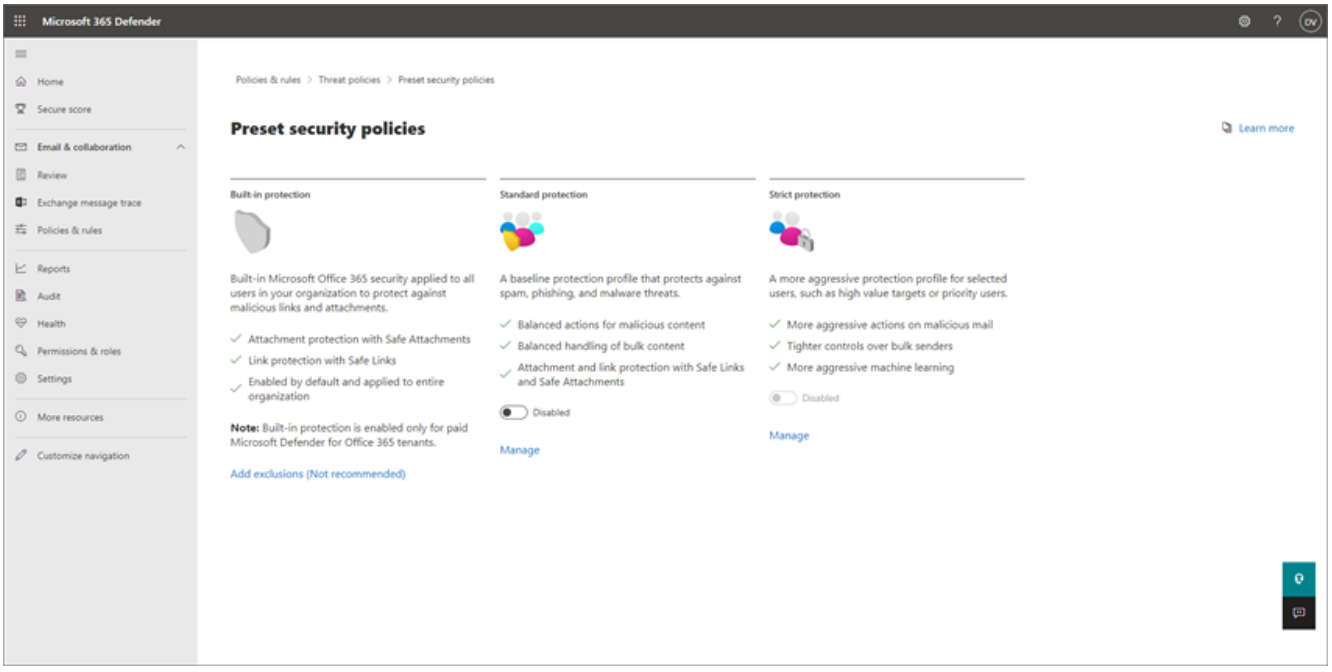

Рис. 2.7. Панель політик безпеки

Попередньо встановлені політики безпеки – це не те саме, що стандартні параметри безпеки. Як правило, спочатку ви використовуєте стандартні

параметри безпеки або умовний доступ, а потім додаєте свої політики безпеки. Попередньо встановлені політики безпеки спрощують процес додавання ваших політик безпеки. Ви також можете додати власні власні політики.

Що таке попередньо встановлені політики безпеки? Попередньо встановлені політики безпеки забезпечують захист електронної пошти та вмісту для спільної роботи. Ці політики складаються з:

профілей, що визначають рівень захисту;

політик (такі як захист від спаму, захисту від зловмисного програмного забезпечення, захисту від фішингу, налаштування підробки, уособлення, безпечні вкладення та безпечні посилання).

Параметри політики (наприклад, групи, користувачі або домени для отримання політик і будь-які винятки). У наведеній нижче таблиці підсумовано рівні захисту та попередньо встановлені типи політики.

Таблиця 2.1

Рівні захисту та попередньо встановлені типи політики

Рівень захисту	**опис**
Стандартний захист (*рекомендується для більшості компаній*)	Стандартний захист використовує базовий профіль, який підходить для більшості користувачів. Стандартний захист включає параметри захисту від спаму, зловмисного програмного забезпечення, захисту від фішингу, налаштування підробки, налаштування уособлення, безпечні посилання та політики безпечних вкладень.
Сувора охорона	Строгий захист включає ті самі види політик, що й стандартний захист, але з більш суворими налаштуваннями. Якщо ваш бізнес має відповідати додатковим вимогам безпеки чи правилам, подумайте про застосування суворого захисту принаймні до ваших пріоритетних користувачів або високоцінних цілей.
Вбудований захист	Захищає від шкідливих посилань і вкладень в електронній пошті. Вбудований захист увімкнено та застосовується до всіх користувачів за замовчуванням.

Ви можете вказати користувачів, групи та домени для отримання

попередньо встановлених політик, а також ви можете визначити певні винятки, але ви не можете змінити самі попередньо встановлені політики. Якщо ви хочете використовувати різні параметри для своїх політик безпеки, ви можете створити власні спеціальні політики відповідно до потреб вашої компанії.

Порядок пріоритету політики. Якщо користувачам призначено кілька політик, для застосування політик використовується порядок пріоритетів. Порядок пріоритету працює таким чином:

суворий захист отримує найвищий пріоритет і перекриває всі інші політики;

стандартний захист;

спеціальна політика безпеки.

Вбудований захист отримує найнижчий пріоритет і замінюється суворим захистом, стандартним захистом і спеціальними політиками.

Строгий захист перекриває всі інші політики, а вбудований захист перекривається іншими політиками.

Ми можемо створюватие власні політики безпеки. Попередньо встановлені політики безпеки, забезпечують надійний захист для більшості підприємств. Однак ви не обмежені використанням лише попередньо встановлених політик безпеки. Ви можете визначити власні політики безпеки відповідно до потреб вашої компанії.

Ми можемо налаштувати власну політику безпеки щодо:

захисту від шкідливих програм;

розширеного захисту від фішингу;

захист від спаму;

безпечнихпосилань та безпечних вкладень.

Другий етап – навчання та тренування співробітників – користувачів.

На цьому етапі налаштовуються некеровані пристрої BYOD (“Bring Your Own Device”), щоб вони стали безпечною частиною всієї екосистеми.

Кожен пристрій є можливим шляхом атаки на вашу мережу, і його необхідно відстежувати та належним чином керувати, навіть ті пристрої, які є особистою власністю, але використовуються для роботи. У цій критично

важливій місії навчіть усіх захищати свої власні пристрої (BYOD). Некеровані пристрої можуть становити загрозу для вашої організації. Важливо допомогти всім якомога швидше захистити свої пристрої.

Нашими цілями є: всім потрібно налаштувати MFA.

Багатофакторна автентифікація (MFA) забезпечує підвищену безпеку, оскільки замість використання лише пароля чи текстового коду для перевірки доступу використовується окрема програма на вашому телефоні. Це ускладнює злом. Коли потрібен MFA, члени організації можуть використовувати програму Microsoft Authenticator для безпечного входу на своїх пристроях.

Необхідно встановити програми Microsoft 365 на пристрої.

Необхідно захистити некеровані пристрої Windows і Mac. Ця мета спрямована на створення захисту для будь-яких некерованих ПК і комп'ютерів Mac з Windows 10, не зареєстрованих у Microsoft Intune. Цілком імовірно, що ваш малий бізнес або кампанія може мати персонал, який приносить власні пристрої (BYOD), і цими пристроями ніхто не керує. BYOD включає особисті телефони, планшети та ПК. Кожен користувач BYOD повинен встановити та запустити програму Company Portal, щоб зареєструвати ці пристрої та отримати доступ до ресурсів компанії.

Дуже важливо переконатися, що ваші перші користувачі дотримуються цих вказівок, щоб мінімальні можливості безпеки були налаштовані на всіх пристроях BYOD.

Необхідно увімкнути шифрування пристрою. Шифрування пристрою доступне на багатьох пристроях Windows і допомагає захистити ваші дані, шифруючи їх. Якщо ви ввімкнете шифрування пристрою, лише авторизовані особи матимуть доступ до вашого пристрою та даних. Якщо шифрування пристрою недоступне на вашому пристрої, замість цього можна ввімкнути стандартне шифрування BitLocker. (BitLocker недоступний у версії Windows 10 Home.)

Необхідно захистити свій пристрій за допомогою безпеки Windows. Якщо у вас Windows 10 або 11, ви отримаєте найновіший антивірусний захист із

функцією безпеки Windows. Коли ви вперше запускаєте Windows 10, безпека Windows увімкнена та активно допомагає захистити ваш ПК шляхом сканування на наявність зловмисного програмного забезпечення (зловмисного програмного забезпечення), вірусів і загроз безпеці. Безпека Windows використовує захист у режимі реального часу для сканування всього, що ви завантажуєте або запускаєте на своєму ПК.

Windows Update автоматично завантажує оновлення для безпеки Windows, щоб захистити ваш комп'ютер від загроз. Якщо у вас попередня версія Windows і ви використовуєте Microsoft Security Essentials, радимо перейти до Windows Security.

Необхідно увімкнути брандмауер Windows Defender. Ви повинні завжди запускати Windows Defender Firewall, навіть якщо у вас увімкнено інший брандмауер. Вимкнення брандмауера Windows Defender може зробити ваш пристрій (і вашу мережу, якщо вона є) більш вразливими до несанкціонованого доступу.

Необхідно захистити всю електронну пошту. Електронна пошта може містити зловмисні атаки, які маскуються під нешкідливі повідомлення. Крім того, системи електронної пошти особливо вразливі, оскільки електронною поштою обробляють усі в організації, а безпека залежить від того, що люди постійно приймають правильні рішення з цими повідомленнями. Для цього необхідно:

захиститися від фішингу та інших атак;

налаштувати зашифровану електронну пошту.

Окрім захисту від атак, який пропонує Microsoft 365 Business Premium, існують інші заходи, яких повинні вжити всі учасники, щоб захистити організацію. Переконайтеся, що всі розуміють такі поняття:

спам або небажана пошта. Є багато причин, чому ви можете отримувати небажані листи, і не всі небажані листи однакові. Однак ви можете зменшити те, що потрапляє до вас, і таким чином зменшити ризики атак, відфільтрувавши небажану пошту;

фішинг. Фішингове шахрайство – це електронний лист, який здається

законним, але є спробою отримати вашу особисту інформацію або викрасти ваші гроші;

спуфінг. Шахраї також можуть використовувати техніку, яка називається спуфінг, щоб створити враження, ніби ви отримали електронний лист від себе;

зловмисне програмне забезпечення – це зловмисне програмне забезпечення, яке можна інсталювати на ваш комп'ютер і зазвичай встановлюється після того, як ви натиснули посилання або відкрили документ із електронного листа. Існують різні типи зловмисного програмного забезпечення (наприклад, програми-вимагачі, коли ваш комп'ютер захоплюють), але ви не хочете мати жодного з них.

Ваші дані та інформація є важливими та часто конфіденційними. Мета тут полягає в тому, щоб допомогти захистити цю конфіденційну інформацію, переконавшись, що всі використовують мітки конфіденційності, щоб одержувачі електронної пошти поводилися з інформацією з максимальною конфіденційністю.

Розглянемо кращі практики.

Перш ніж надсилати електронні листи з конфіденційною або конфіденційною інформацією, їм слід увімкнути:

шифрування: Ви можете зашифрувати свою електронну пошту, щоб захистити конфіденційність інформації в ній. Коли ви шифруєте повідомлення електронної пошти, воно перетворюється з читабельного звичайного тексту на зашифрований текст. Лише одержувач, який має приватний ключ, що збігається з відкритим ключем, використаним для шифрування повідомлення, може розшифрувати повідомлення для читання. Проте будь-який одержувач без відповідного закритого ключа бачить текст, який неможливо розібрати. Ваш адміністратор може визначити правила автоматичного шифрування повідомлень, які відповідають певним критеріям. Наприклад, ваш адміністратор може створити правило, яке шифрує всі повідомлення, надіслані за межі вашої організації, або всі повідомлення, у яких згадуються певні слова чи фрази. Будь-які правила шифрування застосовуватимуться автоматично;

мітки конфіденційності: якщо ваша організація цього вимагає, ви можете налаштувати мітки конфіденційності, які ви застосовуєте до своїх файлів і

електронної пошти, щоб вони відповідали політикам захисту інформації вашої організації. Коли ви встановлюєте мітку, вона зберігається у вашій електронній пошті навіть після її надсилання, наприклад, у вигляді заголовка вашого повідомлення.

Необхідно навчати користувачів безпечному користуванню електронною поштою. Акцентується увага на необхідність звертання уваги на підозрілі листи у своїй електронній пошті та вживання необхідних заходів, щоб захистити себе від атак. Обмін файлами з іншими та безпечна співпраця має здійснюватися з використанням Microsoft Teams, SharePoint і OneDrive.

Необхідно співпрацювати та безпечно ділітися інформацією.

Тепер, коли ви захищені програмами Microsoft 365 Business Premium Microsoft 365, ваша наступна місія – налаштувати безпечний обмін файлами та зв’язок. Найкращий спосіб безпечно співпрацювати та ділитися – використовувати Microsoft Teams. Завдяки Microsoft Teams усі ваші файли та повідомлення перебувають у захищеному середовищі й не зберігаються небезпечними способами за його межами. Ваша організація залежить від захисту ваших даних та інформації, а це означає, що ви хочете захистити свої файли всіма можливими засобами.

Третій етап – захист керованих пристроїв. Це завдання виконує адміністратор безпеки. Він реєструє, налаштовує та захищає керовані пристрої організації, щоб вони контролювалися та захищали від загроз.

Можливості Microsoft Defender для бізнесу, які тепер включені в Microsoft 365 Business Premium, можуть допомогти забезпечити захист пристроїв вашої організації від програм-вимагачів, шкідливих програм, фішингу та інших загроз. Коли ви завершите виконання своїх цілей, ви можете бути впевнені, знаючи, що ви виконали свою частину для захисту вашої організації!

Для цього необхідно:

оновити пристрої Windows під керуванням Windows 7 Pro, Windows 8 Pro або Windows 8.1 Pro до Windows 10 або 11 Pro;

підключити пристрої до Defender for Business і застосовуйте політики

безпеки;

використовуйте Windows Autopilot, щоб установити та конфігурувати нові пристрої або скинути, змінити призначення та відновити пристрої;

установити програми Microsoft 365 на будь-які пристрої, на яких ще не встановлено програми Microsoft 365.

Після досягнення цих цілей ваша загальна місія щодо захисту вашої організації від кібератак та інших загроз кібербезпеці буде успішною. Тепер обов’язково створіть свої групи реагування для вирішення будь-яких ситуацій, які можуть виникнути під час захисту цілісності системи.

Отже, виконання всіх етапів є найефективнішим способом перешкодити хакерам, а також захиститися від програм-вимагачів і допомогти забезпечити майбутнє організації за допомогою Microsoft 365 Business Premium.

Таким чином, Microsoft 365 Business Premium пропонує комплексне рішення для продуктивності та безпеки малого та середнього бізнесу. Адміністратори безпеки забезпечуються необхідними засобами в одному місці для адміністрування та цілодобової підтримки, одночасно зменшуючи витрати та складнощі для бізнесу.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

3.1. Порядок застосування методів та засобів захисту інформаційних ресурсів рішення Microsoft 365 Business Premium

Розглянемо завдання щодо забезпечення безпеки та як вони виконуються в рішенні Microsoft 365 Business Premium відповідно до [12].

1. Щоденні завдання для служби безпеки підприємства.

Перевірте інформаційну панель керування вразливістю:

Отримайте знімок уразливості загроз, подивившись на інформаційну панель керування вразливістю, яка відображає, наскільки ваша організація вразлива до загроз кібербезпеці. Високий показник ризику означає, що ваші пристрої більш вразливі до використання:

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть Vulnerability management > Dashboard.

2. Подивіться на оцінку впливу вашої організації. Якщо він у прийнятному або високому діапазоні, ви можете рухатися далі. Якщо ні, виберіть «Покращити оцінку», щоб переглянути додаткові відомості та рекомендації щодо безпеки для покращення цієї оцінки.

Обізнаність про свій показник впливу допомагає:

швидко зрозуміти та визначити висновки високого рівня щодо стану безпеки у вашій організації;

виявляти та реагувати на сфери, які потребують дослідження або дії для покращення поточного стану;

спілкуйтися з колегами та керівництвом про вплив заходів безпеки.

Перегляньте незавершені дії в Центрі дій:

У міру виявлення загроз починаються дії з усунення. Залежно від конкретної загрози та того, як налаштовано параметри безпеки, дії щодо

виправлення можуть виконуватися автоматично або лише після схвалення, тому їх слід регулярно контролювати. Дії виправлення відстежуються в Центрі дій.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть Action center.

2. Виберіть вкладку «Очікує» , щоб переглянути та схвалити (або відхилити) будь-які дії, що очікують. Такі дії можуть виникати в результаті захисту від вірусів або зловмисного програмного забезпечення, автоматизованих розслідувань, дій вручну або сеансів відповіді в реальному часі.

3. Виберіть вкладку Історія , щоб переглянути список виконаних дій.

Перегляньте пристрої з виявленням загроз.

Коли на пристроях виявляються загрози, ваша команда безпеки має знати про це, щоб можна було негайно вжити будь-яких необхідних дій, наприклад ізоляції пристрою.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть «Звіти» > «Загальні» > «Звіт про безпеку».

2. Прокрутіть униз до рядка Вразливі пристрої. Якщо на пристроях виявлено загрози, ви побачите цю інформацію в цьому рядку.

Дізнайтеся про нові інциденти або сповіщення.

У міру виявлення загроз і спрацьовування сповіщень виникають інциденти. Команда безпеки вашої компанії може переглядати інциденти та керувати ними на порталі Microsoft 365 Defender.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) у навігаційному меню виберіть Інциденти. Інциденти відображаються на сторінці з відповідними сповіщеннями.

2. Виберіть сповіщення, щоб відкрити його спливаючу панель, де можна дізнатися більше про сповіщення.

3. У випадаючому вікні ви можете побачити заголовок сповіщення, переглянути список активів (наприклад, кінцевих точок або облікових записів користувачів), які зазнали впливу, виконати доступні дії та використати посилання для перегляду додаткової інформації та навіть відкрити сторінку

деталей для вибраного сповіщення.

Запустіть сканування або автоматизоване дослідження.

Ваша команда безпеки може ініціювати сканування або автоматичне розслідування на пристрої з високим рівнем ризику або виявлені загрози. Залежно від результатів сканування або автоматизованого дослідження дії з виправлення можуть відбуватися автоматично або після схвалення.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть «Активи» > «Пристрої».

2. Виберіть пристрій, щоб відкрити його розкривну панель, і перегляньте інформацію, яка відображається.

3. Виберіть три крапки (...), щоб відкрити меню дій.

4. Виберіть дію, як-от «Запустити антивірусне сканування» або «Ініціювати автоматичне дослідження».

Щотижневі завдання для вашої служби безпеки.

Відстежуйте та покращуйте свій рейтинг Microsoft Secure.

Microsoft Secure Score – це показник рівня безпеки вашої організації. Вищі цифри вказують на те, що потрібно менше дій щодо покращення. Використовуючи Secure Score, ви можете:

1. Звіт про поточний стан безпеки вашої організації.

2. Поліпште свою безпеку, забезпечивши видимість, видимість, керівництво та контроль.

3. Порівняйте з контрольними показниками та встановіть ключові показники ефективності (KPI).

Щоб перевірити свій бал, виконайте такі дії:

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) на навігаційній панелі виберіть Оцінка безпеки.

2. Перегляньте та прийміть рішення щодо виправлення та дій, щоб покращити загальну оцінку безпеки Microsoft.

Покращте показник безпеки для пристроїв.

Покращуйте конфігурацію безпеки, виправляючи проблеми за допомогою

списку рекомендацій щодо безпеки. Коли ви це робите, ваш показник безпеки Microsoft для пристроїв покращується, а ваша організація стає більш стійкою проти загроз кібербезпеки та вразливостей у майбутньому.

Завжди варто витратити час на перегляд і покращення свого результату.

1. Щоб перевірити свою оцінку безпеки, на порталі Microsoft 365 Defender (https://security.microsoft.com) на панелі навігації виберіть Оцінка безпеки.

2. На картці Microsoft Secure Score for Devices на інформаційній панелі Defender Vulnerability Management виберіть одну з категорій. Відображається список рекомендацій, пов’язаних із цією категорією, а також рекомендації.

3. Виберіть елемент у списку, щоб відобразити деталі, пов’язані з рекомендацією.

4. Виберіть параметри виправлення.

5. Прочитайте опис, щоб зрозуміти контекст проблеми та що робити далі. Виберіть термін виконання, додайте примітки та виберіть Експортувати всі дані про виправлення у CSV , щоб ви могли прикріпити їх до електронного листа для подальших дій. Повідомлення про підтвердження повідомляє, що завдання виправлення створено.

6. Надішліть додатковий електронний лист своєму IT-адміністратору та дайте час, який ви відвели для поширення виправлення в системі.

7. Поверніться до картки Microsoft Secure Score for Devices на інформаційній панелі. У результаті ваших дій кількість рекомендацій щодо засобів контролю безпеки зменшилася.

8. Виберіть Елементи керування безпекою, щоб повернутися до сторінки рекомендацій щодо безпеки. Елемент, який ви вирішували, більше не відображається в списку, що призводить до підвищення рівня безпеки Microsoft.

Щомісячні завдання для служби безпеки підприємства.

Створення звітів.

Кілька звітів доступні на порталі Microsoft 365 Defender (https://security.microsoft.com).

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області

навігації виберіть «Звіти».

2. Виберіть звіт для перегляду. Кожен звіт відображає багато відповідних категорій для цього звіту.

3. Виберіть «Переглянути деталі», щоб переглянути докладнішу інформацію для кожної категорії.

4. Виберіть назву певної загрози, щоб переглянути докладні відомості про неї.

Запустіть посібник із моделювання.

Завжди корисно підвищити рівень безпеки для вас і вашої команди за допомогою навчання. Ви можете отримати доступ до посібників із моделювання на порталі Microsoft 365 Defender. Підручники охоплюють кілька типів кіберзагроз. Щоб почати:

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть Підручники.

2. Ознайомтеся з покроковими інструкціями для підручника, який вам цікавий, а потім завантажте файл або скопіюйте сценарій, потрібний для запуску моделювання відповідно до інструкцій.

Використовуйте навчальний центр, щоб покращити свої знання про загрози кібербезпеці та способи їх усунення. Рекомендується ознайомитися з ресурсами, які пропонуються, особливо в розділах Microsoft 365 Defender і Endpoints.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації виберіть Learning hub.

2. Виберіть область, наприклад Microsoft 365 Defender або Endpoints.

3. Виберіть елемент, щоб дізнатися більше про кожну концепцію.

Завдання, які ваша команда безпеки виконує за потреби.

Використовуйте інформаційну панель аналізу загроз, щоб отримати огляд поточного ландшафту загроз, виділяючи звіти, які найбільше стосуються пыдприэмства.

На порталі Microsoft 365 Defender (https://security.microsoft.com) на навігаційній панелі виберіть Аналітика загроз, щоб відобразити інформаційну

панель аналізу загроз. Інформаційна панель узагальнює загрози в наступних розділах:

останні загрози містять список останніх опублікованих або оновлених звітів про загрози, а також кількість активних і вирішених попереджень;

загрози великого впливу перераховують загрози, які мають найбільший вплив на вашу організацію. У цьому розділі спочатку перераховані загрози з найбільшою кількістю активних і вирішених сповіщень.

Найвищий рівень уразливості містить список загроз із найвищим рівнем уразливості першими. Рівень уразливості загрози розраховується з використанням двох частин інформації: наскільки серйозні вразливості, пов’язані із загрозою, і скільки пристроїв у вашій організації можуть використати ці вразливості.

Виберіть назву того, що ви хочете дослідити, і прочитайте відповідний звіт.

Ви також можете переглянути повний звіт аналітика, щоб отримати докладніші відомості, або вибрати інші заголовки, щоб переглянути пов’язані інциденти, активи, на які вплинуло, а також ризики та пом’якшення.

Виправлення елементів.

Microsoft 365 Business Premium містить кілька дій із виправлення. Деякі дії виконуються автоматично, а інші очікують схвалення команди безпеки.

1. На порталі Microsoft 365 Defender (https://security.microsoft.com) в області навігації перейдіть до Активи > Пристрої.

2. Виберіть пристрій, наприклад із високим рівнем ризику або рівнем впливу. Відкриється спливаюча панель із додатковою інформацією про сповіщення та інциденти, створені для цього елемента.

3. У випадаючому меню перегляньте інформацію, яка відображається. Виберіть три крапки (...), щоб відкрити меню зі списком доступних дій.

4. Виберіть доступну дію. Наприклад, ви можете вибрати «Запустити антивірусну перевірку», що змусить Microsoft Defender Antivirus розпочати швидке сканування на пристрої. Або ви можете вибрати «Ініціювати автоматизоване дослідження», щоб запустити автоматичне дослідження на пристрої.

3.2. Порядок використання Microsoft 365 Business Premium для захисту віддаленої робочої сили

Microsoft 365 Business Premium – це комплексний набір продуктів для співпраці та інструментів безпеки корпоративного рівня, розроблених спеціально для малих і середніх підприємств із кількістю співробітників менше 300 осіб. Він містить додатки Office для підвищення продуктивності, а також розширені можливості безпеки, які допоможуть захистити бізнес від кіберзагроз, дані та пристрої.

Щоб забезпечити безперебійну продуктивність співробітників, які намагаються отримати доступ до бізнес-ресурсів зі своїх домівок, рекомендується підійти до безпеки з точки зору захисту доступу, забезпечення безпеки пристроїв (ПК, Mac і мобільні пристрої) і захисту даних. Microsoft 365 Business Premium забезпечує міцну основу функцій безпеки для цих трьох категорій, які показано на рис. 3.1.

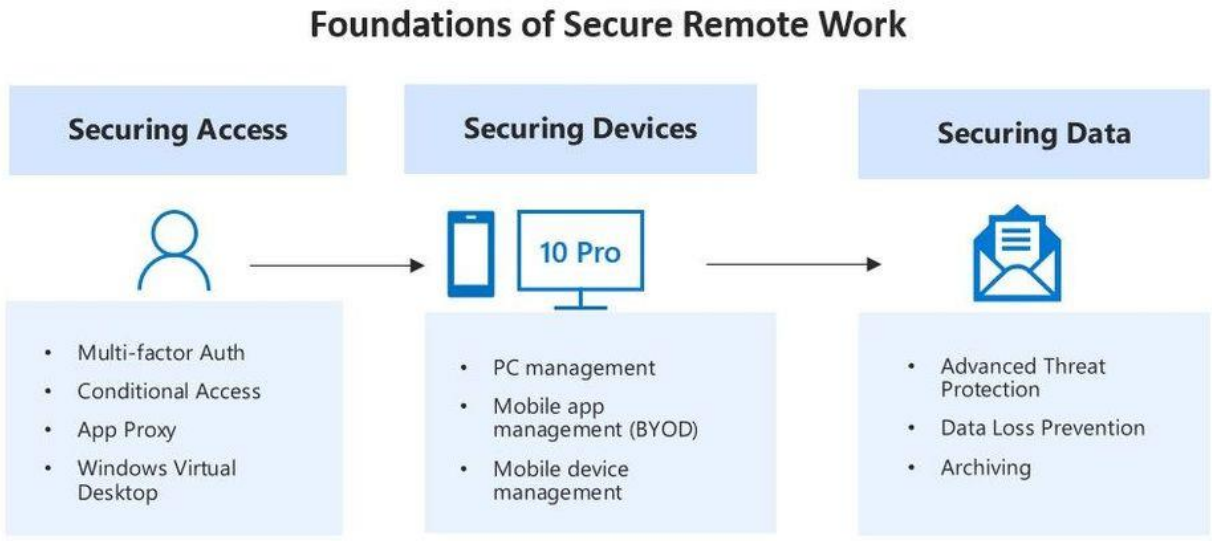

Рис. 3.1. Основи захисту віддаленої робочої сили [8]

Розглянемо даний підхід більш детальніше.

1. Захист доступу. Одним із найважливіших аспектів уможливлення сценаріїв роботи з дому є забезпечення того, щоб користувачі могли віддалено

отримувати доступ до систем у безпечний спосіб – з будь-якого місця та з будь-якого пристрою. Наведені нижче функції в Microsoft 365 Business Premium допоможуть вам це зробити. Ви можете ввімкнути деякі з них або всі залежно від потреб вашої організації:

багатофакторна автентифікація (MFA): це покращує безпеку, вимагаючи більше одного методу автентифікації для перевірки особи користувача під час входу в системи або дані вашої компанії. Наприклад, користувач повинен ввести код або відповісти на телефонний дзвінок, окрім входу за допомогою свого імені користувача та пароля. Цей додатковий рівень перевірки гарантує, що особи, які не є співробітниками, не зможуть отримати доступ до вашого середовища, навіть якщо ім'я користувача та пароль зламано, наприклад, під час фішингової атаки;

умовний доступ: ця функція допомагає контролювати доступ до вашого середовища на основі місцезнаходження, програми, стану пристрою та стану користувача. Наприклад, ви можете створити політику, яка блокує доступ, коли хтось намагається ввійти з країни, у якій ви не ведете бізнес. Або ви можете використовувати умовний доступ, щоб обмежити доступ, якщо користувач входить із нерозпізнаної та потенційно скомпрометованої пристрій. Умовний доступ дає вам можливість захистити доступ на основі кількох критеріїв, а не просто покладатися на ім'я користувача та пароль;

проксі-сервер додатків Azure AD: багато компаній мають критично важливі для бізнесу програми, що працюють локально, до яких немає доступу ззовні корпоративної мережі. Проксі-сервер програми Azure AD дозволяє публікувати ці програми за межами мережі. Це легкий агент, який надає доступ до Інтернету вашим локальним програмам, не відкриваючи широкий доступ до вашої мережі;

віртуальний робочий стіл Windows (WVD): якщо у вас є програми з конфіденційною інформацією, як-от медична чи фінансова інформація, і ви хочете переконатися, що користувачі, які працюють з дому, мають безпечний доступ до даних, ви можете легко ввімкнути цей сценарій, використовуючи WVD. WVD створює віртуальний робочий стіл для віддаленого доступу користувачів. Співробітники можуть отримати доступ до цієї інформації лише в цьому

віддаленому віртуалізованому сеансі та не можуть зберігати жодні дані на своїх локальних робочих станціях;

2. Захист пристроїв. Співробітники використовують широкий спектр ноутбуків, настільних комп'ютерів і мобільних пристроїв для доступу до даних компанії та виконання роботи протягом цього часу. Проблема полягає в тому, щоб захистити всі ці пристрої, оскільки люди використовують їх для роботи з конфіденційною інформацією. Microsoft Intune входить до Microsoft 365 Business Premium і може допомогти керувати ПК і мобільними пристроями. Ось як:

керування комп'ютерами за допомогою Intune: щоб підтримувати безпеку, співробітники повинні постійно оновлювати свої робочі пристрої за допомогою останніх оновлень безпеки, поки вони перебувають за межами вашої корпоративної мережі. Intune може не тільки підтримувати ці пристрої в актуальному стані, але й допомагає повністю керувати вашими ПК за допомогою таких функцій, як застосування політик безпеки або віддалене видалення даних із пристроїв. У Microsoft 365 Business Premium ви можете застосувати попередньо налаштовані політики пристроїв для ПК з Windows 10, які отримують доступ до вашого середовища, наприклад увімкнути Microsoft Defender AV і захист від програм-вимагачів для критичних папок;

керування мобільними пристроями за допомогою Intune: Intune також допомагає вам керувати мобільними пристроями та дає вам гнучкість у виборі того, скільки контролю ви хочете здійснювати над мобільними пристроями, які отримують доступ до середовища вашої компанії. У ситуації Bring-You-Own-Devices (BYOD), коли співробітники використовують особисті мобільні пристрої, ви можете не потрібний повний контроль над особистим пристроєм користувача, але все одно можете захотіти захистити дані компанії, до яких користувач має доступ. У цьому випадку ви можете використовувати політики захисту програм Intune, щоб захистити дані компанії (електронну пошту, команди та OneDrive) на пристрої. Однак, якщо вам потрібен повний контроль над мобільним пристроєм користувача, ви можете «зареєструвати» пристрій у Intune Mobile Device Management і повністю контролювати налаштування пристрою та встановити

політики безпеки;

політики захисту додатків Intune: ці політики дозволяють забороняти користувачам копіювати, вставляти або зберігати корпоративні дані та документи з програм Office для мобільних пристроїв у особистих програмах або місцях зберігання – без будь-якої реєстрації пристрою. Наприклад, за наявності цих політик користувач не може зберегти електронну таблицю даних клієнтів у своїх особистих файлах. Оскільки корпоративні дані зберігаються в затверджених програмах і розташуваннях, у разі втрати або викрадення персонального пристрою ви можете вибірково стерти цю інформацію, не впливаючи на особисті фотографії, програми та дані. Ці політики легко активувати через консоль адміністрування Microsoft 365 Business Premium;

керування мобільними додатками Intune: якщо ви хочете застосувати більш жорсткі політики мобільних пристроїв, які виходять за межі політик захисту програм, ви можете ввімкнути повні можливості керування мобільними пристроями в Intune. Тоді ви зможете застосовувати глибокі політики безпеки, орієнтовані на пристрій, наприклад блокування знімків екрана. Цей підхід вимагає процесу реєстрації пристрою для пристроїв iOS або Android.

3. Захист даних. Іншим важливим кроком у створенні сценаріїв віддаленої роботи є забезпечення захисту даних компанії. Оскільки кіберзлочинці коригують свою тактику, щоб скористатися поточною ситуацією, доцільно активувати політики для захисту від кіберзагроз і запобігання фішингу. Також важливо забезпечити захист конфіденційних даних, таких як номери соціального страхування, дані кредитних карток клієнта та ідентифікаційну інформацію (PII), а також наявність політик для контролю доступу та обміну.

Розширений захист від загроз Office 365: нещодавній звіт Microsoft Security Research свідчить про сплеск щоденного зловмисного програмного забезпечення та спаму, які використовують приманки для COVID-19. Office 365 ATP допомагає захистити ваш бізнес від складних атак фішингу та програм-вимагачів на електронну пошту, OneDrive та Teams, спрямованих на компрометацію інформації про співробітників або клієнтів. Office 365 ATP захищає вас такими

способами:

складне сканування вкладень в електронній пошті, OneDrive та Teams, яке використовує аналіз на основі штучного інтелекту для виявлення та відхилення небезпечних повідомлень;

автоматична перевірка посилань в електронній пошті, документах і Teams, щоб визначити, чи є вони частиною фішингової схеми, і запобігти доступу користувачів до небезпечних веб-сайтів;

інтелектуальні засоби захисту від спуфінгу, щоб застерегти вас від видавання себе за домен, який має на меті змусити користувачів подумати, що електронний лист надходить від організації всередині організації.

Запобігання втраті даних (DLP): якщо ви стурбовані підвищеним ризиком того, що працівники помилково нададуть конфіденційну інформацію під час роботи вдома, ця функція допоможе вам ідентифікувати, контролювати та захистити конфіденційну інформацію від ненавмисного поширення через електронну пошту або в документах. DLP виявляє певні типи конфіденційної інформації, яка передається особам за межами вашої організації, як-от номери кредитних карток, державні ідентифікатори, дати народження та навіть ідентифікаційна інформація для певної країни.

Онлайн-архівація Exchange: це допомагає зберігати всі дані компанії в безпеці, зберігаючи їх на випадок втрати/викрадення пристроїв, збою інфраструктури або для виконання судових процесів і зобов’язань щодо відповідності. Онлайн-архівація Exchange захищає дані, дозволяючи легко архівувати повідомлення та документи та мати доступ до них у будь-який час/у будь-якому місці. Він зберігає інформацію користувача, включаючи видалені елементи, для електронного виявлення або відновлення пізніше.

3.3. Рекомендації щодо захисту інформаційних ресурсів для малого та середнього бізнесу

Інтернет дозволяє підприємствам будь-якого розміру та з будь-якого місця

виходити на нові та більші ринки та надає можливості працювати ефективніше за допомогою комп'ютерних інструментів. Незалежно від того, чи планує компанія запровадити хмарні обчислення чи просто використовувати електронну пошту та підтримувати веб-сайт, кібербезпека має бути частиною плану. Крадіжка цифрової інформації стала найпоширенішим шахрайством, перевершивши фізичну крадіжку. Кожен бізнес, який використовує Інтернет, несе відповідальність за створення культури безпеки, яка підвищить довіру бізнесу та споживачів [6].

Широкосмуговий зв'язок та інформаційні технології є потужними чинниками, які допомагають малому та середньому бізнесу вийти на нові ринки та підвищити продуктивність і ефективність. Однак компаніям потрібна стратегія кібербезпеки, щоб захистити свій власний бізнес, клієнтів і дані від зростаючих загроз кібербезпеці [6]. Розглянемо її основні складові:

1. Навчіть співробітників принципам безпеки.

Встановіть базові практики та політику безпеки для співробітників, наприклад вимогу до надійних паролів, і встановіть відповідні вказівки щодо користування Інтернетом, які детально описують покарання за порушення політики кібербезпеки компанії. Встановіть правила поведінки, що описують, як обробляти та захищати інформацію про клієнтів та інші важливі дані.

2. Захист інформації, комп'ютерів і мереж від кібератак.

Тримайте машини в чистоті: найновіше програмне забезпечення безпеки, веб-браузер і операційна система є найкращим захистом від вірусів, зловмисного програмного забезпечення та інших онлайн-загроз. Налаштуйте антивірусне програмне забезпечення на сканування після кожного оновлення. Встановлюйте інші ключові оновлення програмного забезпечення, щойно вони стануть доступними.

3. Забезпечте безпеку брандмауера для підключення до Інтернету.

Брандмауер – це набір пов'язаних програм, які запобігають доступу сторонніх осіб до даних у приватній мережі. Переконайтеся, що брандмауер операційної системи ввімкнено, або встановіть безкоштовне програмне

забезпечення брандмауера, доступне в Інтернеті. Якщо співробітники працюють вдома, переконайтеся, що їх домашні системи захищені брандмауером.

4. Створіть план дій із захисту мобільного пристрою.

Мобільні пристрої можуть створювати значні проблеми з безпекою та керуванням, особливо якщо вони містять конфіденційну інформацію або мають доступ до корпоративної мережі. Вимагайте від користувачів захисту паролем своїх пристроїв, шифрування даних і встановлення додатків безпеки, щоб запобігти крадіжці інформації зловмисниками, коли телефон знаходиться в загальнодоступних мережах. Обов'язково встановіть процедури звітування про втрачене або викрадене обладнання.

5. Зробіть резервні копії важливих бізнес-даних.

Регулярно створюйте резервні копії даних на всіх комп'ютерах. До критично важливих даних належать документи для обробки текстів, електронні таблиці, бази даних, фінансові файли, кадрові файли та файли дебіторської/кредиторської заборгованості. Робіть резервні копії даних автоматично, якщо це можливо, або принаймні щотижня та зберігайте копії поза сайтом або в хмарі.

6. Контролюйте фізичний доступ до своїх комп'ютерів і створюйте облікові записи користувачів для кожного співробітника.

Запобігайте доступу чи використанню бізнес-комп'ютерів неавторизованими особами. Ноутбуки можуть бути особливо легкою мішенню для крадіжки або можуть бути втрачені, тому замикайте їх, коли вони залишаються без нагляду. Переконайтеся, що для кожного співробітника створено окремий обліковий запис користувача та вимагайте надійних паролів. Адміністративні привілеї слід надавати лише довіреному IT-персоналу та ключовому персоналу.

7. Захистіть свої мережі Wi-Fi.

Якщо на вашому робочому місці є мережа Wi-Fi, переконайтеся, що вона безпечна, зашифрована та прихована. Щоб приховати свою мережу Wi-Fi, налаштуйте безпроводову точку доступу або маршрутизатор так, щоб вона не

транслювала назву мережі, відому як ідентифікатор набору послуг (SSID). Захистить доступ до роутера паролем.

8. Використовуйте найкращі практики щодо платіжних карток.

Співпрацюйте з банками або процесорами, щоб забезпечити використання найбільш надійних і перевірених інструментів і служб боротьби з шахрайством. Ви також можете мати додаткові зобов'язання щодо безпеки відповідно до угод із вашим банком або процесором. Ізолюйте платіжні системи від інших, менш безпечних програм і не використовуйте один і той же комп'ютер для обробки платежів і перегляду Інтернету.

9. Необхідно обмежити доступ співробітників до даних, обмежити повноваження щодо встановлення програмного забезпечення.

Не надавайте жодному співробітнику доступ до всіх систем даних. Співробітникам слід надавати доступ лише до певних систем даних, які їм потрібні для роботи, і не можна встановлювати будь-яке програмне забезпечення без дозволу.

10. Використовуйте надійні паролі та автентифікацію.

Вимагайте від працівників використовувати унікальні паролі та змінювати паролі кожні три місяці. Розгляньте можливість впровадження багатофакторної автентифікації, яка потребує додаткової інформації, крім пароля, для входу. Зверніться до своїх постачальників, які обробляють конфіденційні дані, особливо фінансових установ, щоб дізнатися, чи пропонують вони багатофакторну автентифікацію для вашого облікового запису.

Кіберінциденти різко почастішали серед малих підприємств, які часто не мають ресурсів для захисту від руйнівних атак, таких як програми-вимагачі [5]. Кібербезпека стосується культури так само, як і технологій. Більшість організацій потрапляють у пастку, думаючи, що лише IT-команда відповідає за безпеку. У результаті вони роблять типові помилки, які збільшують шанси на компроміс. Культуру не можна делегувати. Керівники відіграють важливу роль, виконуючи такі завдання. Тому, вони мають:

сформувати культуру безпеки. Зверніть увагу на те, щоб говорити про

кібербезпеку безпосередньо підлеглим і всій організації. Якщо ви регулярно спілкуєтеся електронною поштою з персоналом, додайте оновлення щодо ініціатив програми безпеки. Коли ви встановлюєте квартальні цілі разом зі своєю командою керівництва, включайте важливі цілі безпеки, які відповідають бізнес-цілям. Безпека має бути «щоденною», а не випадковою діяльністю. Наприклад, встановіть цілі щодо покращення безпеки ваших даних і облікових записів за допомогою впровадження багатофакторної автентифікації (MFA), кількості систем, які ви повністю виправили, і кількості систем, для яких ви створюєте резервні копії;

виберіть і підтримуйте «Менеджера програми безпеки». Цій людині не обов'язково бути фахівцем із безпеки чи навіть IT-фахівцем. Менеджер програми безпеки гарантує, що ваша організація реалізує всі ключові елементи потужної програми кібербезпеки. Керівник повинен звітувати вам та іншим керівникам вищої ланки про прогрес і перешкоди принаймні щомісяця або на початку частіше;

перегляньте та затвердіть План реагування на інциденти (IRP). Керівник програми безпеки створить письмовий IRP для перегляду керівництвом. IRP – це ваш план дій до, під час і після інциденту безпеки. Приділяйте йому належну увагу в «мирний час» і залучайте керівників з усієї організації, а не лише служби безпеки та IT. Під час інциденту не буде часу переосмислювати і доопрацьовувати його.

Керівник програми безпеки має проводити регулярні тренування з моделювання атак, які називаються тренуваннями. Ці вправи допоможуть вам і вашій команді виробити рефлекси, які вам знадобляться під час інциденту. Переконайтеся, що ваші старші керівники присутні та беруть участь.

Підтримка генерального директора є надзвичайно важливою, особливо там, де програма безпеки потребує допомоги кожного співробітника. Візьміть на себе відповідальність за певні зусилля замість того, щоб просити про це IT. Наприклад, не покладайтеся на IT-команду, щоб переконати зайнятих співробітників, що вони повинні активувати другий спосіб входу в свою електронну пошту, увімкнувши

MFA. Натомість зробіть повідомлення про МЗС персоналу самостійно та відстежуйте прогрес. Особисто зв’яжіться з людьми, які не ввімкнули MFA. Це створює культуру безпеки зверху.

Використання MFA захищає обліковий запис не тільки за допомогою імені користувача та пароля. Користувачі, які ввімкнули MFA, мають набагато менше шансів бути зламаними.

Керівнику програми безпеки потрібно керувати елементами програми безпеки, інформувати генерального директора про прогрес і перешкоди, а також давати рекомендації. Ось найважливіші завдання менеджера програми безпеки:

навчання. Увесь персонал має пройти офіційне навчання, щоб розуміти зобов’язання організації щодо безпеки, які завдання вони повинні виконувати (наприклад, увімкнути MFA, оновлювати програмне забезпечення та уникати натискання підозрілих посилань, які можуть бути фішинговими атаками), і як посилити підозрілу активність;

створення та дотримання Плану реагування на інциденти (IRP). У IRP буде вказано, що організація має робити до, під час і після фактичного чи потенційного інциденту безпеки. Він включатиме ролі та обов’язки для всіх основних дій, а також адресну книгу для використання, якщо мережа не працює під час інциденту. Попросіть генерального директора та інших керівників офіційно затвердити це. Переглядайте його щокварталу та після кожного інциденту з безпекою або «незабаром»;

застосування MFA. Найважливішим кроком, який може зробити організація, є переконатися, що всі співробітники використовують MFA для входу в ключові системи, особливо електронну пошту. Хоча це завдання також зазначено в розділі IT нижче, дуже важливо, щоб кілька людей регулярно переглядали статус MFA;

патчінг. Багато атак вдаються, тому що жертви використовували вразливе програмне забезпечення, коли була доступна новіша, безпечніша версія. Підтримуйте виправлення систем – це один із найбільш рентабельних методів покращення рівня безпеки;

створення резервних копій. Багато організацій, які стали жертвами програм-

вимагачів, або не мали резервних копій, або мали неповні/пошкоджені резервні копії. Недостатньо запланувати регулярне резервне копіювання всіх важливих систем. Дуже важливо регулярно тестувати часткові та повні відновлення. Вам потрібно буде вибрати частоту резервного копіювання (безперервне, щогодини, щотижня тощо). Ви також захочете написати план реставрації. Деякі організації, які зазнали атак програм-вимагачів, виявили, що час відновлення їхніх даних був значно довшим, ніж очікувалося, що вплинуло на їхній бізнес;

роль адміністратора з ноутбуків користувачів. Поширеним вектором атаки є змусити користувачів запустити зловмисне програмне забезпечення. Робота зловмисника полегшується, якщо користувачі мають права адміністратора. Користувач без прав адміністратора не може інсталювати програмне забезпечення, і цей тип атаки не працюватиме;

застосування шифрування диска для ноутбуків. Сучасні смартфони шифрують своє локальне сховище, як і Chromebook. Однак ноутбуки Windows і Mac повинні бути налаштовані на шифрування своїх дисків. Враховуючи, скільки ноутбуків втрачається або викрадається щороку, важливо переконатися, що ваш парк ноутбуків захищений.

Окрім впровадження рішень на основі програмного забезпечення, малим підприємствам слід застосувати певні найкращі технологічні практики та політики для усунення вразливостей безпеки. Існує більше десятка способів захисту пристроїв і мережі бізнесу, а також зростає кількість методів безпечного обміну файлами. Навіть якщо вас зламали, ви можете відновитися після витоку даних.

Оскільки загрози продовжують розвиватися, змінюватимуться й способи боротьби з ними. Ні в якому разі не можна заспокоюватися чи застосовувати недбалий підхід до захисту свого бізнесу, але, як випливає з цього слова, кібербезпека створена для того, щоб підтримувати цифрову безпеку бізнесу. Тож будьте впевнені: якщо ви будете дотримуватись найкращих практик, ваша компанія, ймовірно, буде кращою.

ВИСНОВКИ

В роботі досліджено проблему захисту інформаційних ресурсів для малого та середнього бізнесу, визначено його мету та завдання. Малий і середній бізнес дуже часто не в змозі ефективно протидіяти кібератакам, оскільки таким клієнтам бракує ресурсів, коштів або спеціалізованої допомоги. Утім, вони потребують таких самих надійних технологій захисту, як і великі організації.

Проаналізовано підходи до захисту інформаційних ресурсів для малого та середнього бізнесу. Малі та середні підприємства, які хочуть забезпечити свої мережі принаймні шансами протистояти багатьом атакам, повинні бути готові встановити базове програмне забезпечення безпеки.

Проведено аналіз існуючих технологій захисту інформаційних ресурсів для малого та середнього бізнесу. Досліджено методи та засоби захисту інформаційних ресурсів рішення Microsoft 365 Business Premium.

Microsoft 365 Business Premium – це комплексне хмарне рішення для продуктивності й безпеки, розроблене та створене для малого та середнього бізнесу (до 300 співробітників).

Розглянуто призначення та основні функції рішення Microsoft Defender for Business. Defender for Business – це нове рішення для захисту кінцевих точок, розроблене спеціально для малого та середнього бізнесу. За допомогою цього рішення безпеки кінцевих точок пристрої підприємства краще захищені від програм-вимагачів, шкідливих програм, фішингу та інших загроз.

Розглянуто зміст технології захисту інформаційних ресурсів в Microsoft 365 Business Premium. Основними етапами даної технології є захист середовища інформаційних ресурсів організації, навчання та тренування співробітників – користувачів та захист керованих пристроїв.

На основі досліджень проведених в роботі розглянуто порядок застосування методів та засобів захисту інформаційних ресурсів рішення Microsoft 365 Business Premium, а також порядок використання Microsoft 365 Business Premium для

захисту віддаленої робочої сили.

Розроблено рекомендації керівникам та фахівцям з кібербезпеки щодо захисту інформаційних ресурсів для малого та середнього бізнесу.

Таким чином, правильний захист інформаційних ресурсів для малого та середнього бізнесу має забезпечити конфіденційність, цілісність та доступність корпоративних даних та кібербезпеку інформаційної системи підприємств малого та середнього бізнесу в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Small Business Cyber Security in 2022. Check Point. [Електронний ресурс] – Режим доступу: https://www.checkpoint.com/cyber-hub/cyber-security/small-business-cyber-security-in-2022/.

2. Microsoft 365 Business Premium – productivity and cybersecurity for small business. Article 28/09/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/microsoft-365/business-premium/?view=o365-worldwide.

3. Help protect yourself and your campaign from digital threats. Microsoft. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/microsoft-365/business-premium/m365-campaigns-setup?view=o365-worldwide.

4. Andrew Martins. Cyberattacks and Your Small Business: A Primer for Cybersecurity. Business News Daily Staff. Updated Jun 29, 2022. [Електронний ресурс] – Режим доступу: https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html.

5. CYBER GUIDANCE FOR SMALL BUSINESSES. CISA. [Електронний ресурс] – Режим доступу: https://www.cisa.gov/small-business.

6. Cybersecurity for Small Businesses. [Електронний ресурс] – Режим доступу: https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses.

7. Microsoft Defender for Business. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/?view=o365-worldwide.

8. Ashanka Iddya. Using Microsoft 365 Business Premium to secure your remote workforce. Published Apr 10 2020. [Електронний ресурс] – Режим доступу: https://techcommunity.microsoft.com/t5/small-and-medium-business-blog/using-microsoft-365-business-premium-to-secure-your-remote/ba-p/1298623.

9. 15 Cybersecurity Tools for Small and Medium Businesses (SMBs). Fortinet.

[Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/smb-cybersecurity-tools.

10. Cyber Security Practices and Solutions of interest to SMBs. Ofofo. [Електронний ресурс] – Режим доступу: https://blog.ofofo.io/cybersecurity-practices-and-solutions-of-interest-to-smbs-a-business-perspective-a2e2f5236d1a.

11. Simon Worsfold. Small Business Insights: Inflation now the No.1 concern for small businesses. April 13, 2022. [Електронний ресурс] – Режим доступу: https://quickbooks.intuit.com/r/trends/insights-april-2022/.

12. Microsoft 365 Business Premium security operations guide. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-security-incident-quick-start?view=o365-worldwide.

13. Корж В. І. Технологія захисту інформаційних ресурсів для малого або середнього бізнесу на базі Microsoft 365 Business Premium. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 11-14. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)