УДК 004.05 **DOI:10.30837/rt.2024.3.218.01**

В.І. ЄСІН, д-р техн. наук, В.В. ВІЛІГУРА, Д.Ю. УЗЛОВ, канд. техн. наук

АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ: ПРОБЛЕМИ ТА РЕКОМЕНДАЦІЇ ЩОДО УСПІШНОГО ВПРОВАДЖЕННЯ

Вступ

Протягом останніх десятиліть підприємства активно переходять на цифрові технології. Сьогодні вони підтримують хмарні технології, частіше використовують віддалену роботу, додають рішення на кшталт «як послуга» (as-a-service), а також здійснюють безліч інших важливих перетворень, що призводить до розширення існуючої IT-інфраструктури підприємства. Все більше і більше пристроїв (у тому числі CYOD та BYOD) та сервісів обмінюються інформацією всередині корпоративних мереж, а також за їх межами. Ці зміни призводять до появи нових складних вимог до мережевої безпеки, яким існуючі рішення слабо відповідають [1]. У цих умовах фахівці з безпеки відповідно до нових потреб змушені масштабувати систему мережевої безпеки, часто посилюючи захист шляхом сегментування мережі на дрібніші частини. На жаль, таке рішення створило більше сприятливих можливостей для зловмисників через появу додаткового набору вразливостей, з яким не в змозі впоратися навіть новим, ефективнішим засобам захисту з підвищеним рівнем контролю, через те, що їхнє застосування обмежується межею корпоративної мережі та не дозволяє контролювати те, що відбувається за її межами. Як відомо, традиційна безпека мережі фокусується на захисті периметра. Отримуючи доступ до облікових даних користувача, зловмисники можуть переміщатися по мережі, розповсюджуючи шкідливе програмне забезпечення та додаючи привілеї в міру свого переміщення [2]. Недоліки цього підходу стають очевидними, якщо врахувати, що зловмисники у разі компрометації суб'єктів (кінцевих користувачів, застосунків та інших нефізичних сутностей) можуть отримати доступ до ресурсів усередині або за межами мережі. Більше того, багато підприємств більше не мають чітко визначеного периметра. Периметр втрачає свою актуальність через кілька факторів, включаючи зростання застосування хмарних технологій, мобільність та використання віддалених працівників [3]. Крім того, слід враховувати, що загрозу становлять і внутрішні зловмисники – інсайдери. Таким чином, ідея про те, що жодна мережа (ні внутрішня, ні зовнішня) не заслуговує на довіру, просувається як у наукових колах, так і на практиці [1].

Щоб сьогодні захистити сучасне цифрове підприємство, необхідна комплексна стратегія для безпечного доступу у будь-який час і в будь-якому місці до власних корпоративних ресурсів (застосунків, застарілих / успадкованих систем, даних, пристроїв тощо) незалежно від того, де вони розташовані [4]. Тому підприємства стали переосмислювати традиційний периметр безпеки мережі, схиляючись до нової концепції та архітектури захисту [5].

Такою концепцією є парадигма безпеки, що отримала назву «нульова довіра» (Zero Trust – ZT). Концепція нульової довіри стала дуже популярним підходом до створення захищених систем, що просувається промисловістю та державними органами як новий спосіб створення систем з високим ступенем безпеки [6]. За своєю суттю «нульова довіра» – це філософія, підхід та набір керівних принципів кібербезпеки, що використовуються для створення стратегії, яка фокусується на переміщенні захисту мережі від широких статичних периметрів мережі до вужчого зосередження уваги на суб'єктах, активах підприємства (пристроях, компонентах інфраструктури, застосунках, віртуальних та хмарних компонентах) та окремих або невеликих групах ресурсів [3, 7, 8]. Ідея концепції нульової довіри виникла ще на початку розвитку безпечних обчислень [1]. В її основі лежить застосування принципів безпечного проєктування, взятих із класичної роботи Saltzer та Schroeder [9] и более поздних работ [6, 10, 11], серед яких слід відзначити повне посередництво (перевіряйте кожен доступ на наявність повноважень), відкрите проєктування (розробка не повинна бути закритою; механізми захисту повинні залежати не від безграмотності потенційних зловмисників, а від володіння певними ключами або паролями, що легко захищаються; не повинно бути «безпеки через невідомість»), найменші привілеї (компоненти повинні мати не більше повноважень, ніж їм потрібно), глибокий захист, багаторівневий захист. Особливістю концепції нульової довіри можна вважати додатковий, більш жорсткий принцип «ніколи не довіряти, завжди перевіря-

ти» [12]. При цьому, якщо «*нульова довіра*» являє собою набір концепцій та ідей, розроблених для мінімізації невизначеності в застосуванні точних рішень щодо доступу з найменшими привілеями для кожного запиту в інформаційних системах і службах / сервісах, коли мережу вважають скомпрометованою, то *архітектура нульової довіри* (ZTA – zero trust architecture; іноді в перекладі можна зустріти назву – архітектура з нульовою довірою або архітектура безпеки з нульовою довірою), відповідно до визначення NIST [8] – це план кібербезпеки підприємства, який використовує концепції нульової довіри та охоплює зв'язки компонентів, планування робочого процесу та політики доступу; це архітектура кібербезпеки підприємства, яка базується на принципах нульової довіри та призначена для запобігання витоку даних і обмеження внутрішнього бічного (горизонтального) руху (переміщення). На відміну від архітектури, орієнтованої на захист по периметру, в якій будь-який об'єкт усередині заданого периметра вважається довіреним, ZTA забезпечує обробку будь-якого запиту та надання ресурсу суб'єкту, не покладаючись на неявну довіру [13]. Архітектура нульової довіри враховує нові тенденції, приділяючи особливу увагу захисту ресурсів, а не периметру мережі, оскільки розташування мережі більше не розглядається як основний компонент забезпечення безпеки, необхідної для ресурсу [3, 8]. В рамках архітектури нульової довіри доступ до ресурсів не надається до тих пір, поки суб'єкт, актив або робоче навантаження не будуть верифіковані за допомогою процедур автентифікації та прав / дозволів на виконання певних дій (авторизації) [3]. Тобто в основі архітектури нульової довіри лежить керування ідентифікацією, активами, автентифікація застосунків, сегментація мережі, політики, механізми та фактори аналізу загроз [14].

Одним із факторів, що визначають потребу в ZTA, є складність та гетерогенність сучасних IT-систем [6]. Тому ідея про те, що для забезпечення безпеки системи потрібне повсюдне, детальне та безперервне розгортання багаторівневих засобів контролю безпеки, є цілком очевидною.

Однак незважаючи на популяризацію концепції нульової довіри та очевидні переваги у сфері безпеки від її застосування на підприємствах виникають певні складнощі щодо її реалізації [5, 15, 16-19]. Розгортання архітектури нульової довіри є досить складним як з технічної, так і з організаційної точки зору [18]. Можна відзначити кілька основних перешкод на шляху створення систем нульової довіри в державних і приватних комп'ютерних системах [18, 19]: застарілі системи та інфраструктуру часто неможливо оновити до рівня нульової довіри; навіть якщо оновлення можливе, воно обійдеться недешево; однорангові технології не відповідають концепції нульової довіри, оскільки вони покладаються переважно на паролі, а не на багатофакторну автентифікацію в режимі реального часу; перенесення інформаційних систем організації з власних комп'ютерів на хмарні сервіси може стимулювати розвиток нульової довіри, але тільки в тому випадку, якщо все буде зроблено справді коректно (організації повинні знати, як планувати забезпечення безпеки на основі концепції нульової довіри під час переходу до хмарного середовища, а не простого здійснювати перенесення існуючих додатків у хмару). Крім того, основними серйозними факторами, що перешкоджають впровадженню концепції нульової довіри, за даними звіту компанії Fortinet [15], стали брак інформації для вибору рішення з нульовою довірою та відсутність кваліфікованих розробників/постачальників. У публікаціях галузевих видань технічні аспекти подібних систем описуються нечітко, ігноруються накопичені раніше знання у сфері безпеки, а звіти, що описують реальний досвід створення та використання архітектур нульової довіри, вельми нечисленні. Деякі постачальники IT-послуг стверджують, що вони мають способи реалізації ZTA, але вони не надають подробиць про те, як це зробити. У технічних документах (white papers) цих компаній описуються їх підходи, але вони надають лише високорівневі огляди або списки специфікацій [6]. Ця проблема посилюється ще й тим, що архітектура нульової довіри передбачає використання детального контролю безпеки, тому з великою ймовірністю можна припустити, що доведеться визначати, впроваджувати, розгортати та керувати величезною кількістю політик [18], а знань та досвіду може виявитися недостатньо.

Як видно з викладеного, існує проблема, пов'язана з певним дефіцитом поінформованості про концепцію та архітектуру нульової довіри (про їх теоретичну та практичну значущість) для вибору правильного рішення при побудові системи безпеки корпоративної інфор-

маційної системи підприємства у сучасних умовах. Стаття націлена на вирішення цієї проблеми шляхом узагальнення наявних досліджень та досвіду різних міжнародних компаній, які впроваджують даний підхід на практиці. У ній у стислому викладі розглядаються концептуальна архітектура нульової довіри, її основні логічні компоненти, моделі розгортання ZTA, загрози, пов'язані з архітектурою нульової довіри, а також деякі рекомендації щодо успішного впровадження архітектури нульової довіри на IT-підприємстві, які допоможуть зрозуміти фундаментальні зміни у підході до інформаційної безпеки, кібербезпеки.

1. Архітектура нульової довіри

Архітектура нульової довіри сьогодні це концепція, що розвивається, для якої поки не існує ні сертифікації, ні практичних стандартів [2]. Хоча робота у цьому напрямі активно проводиться. Що стосується нормативних документів, то на сьогодні є основна спеціальна публікація NIST SP 800-207 (в цьому документі дається абстрактне визначення архітектури нульової довіри, наводяться загальні моделі розгортання та варіанти використання, в яких нульова довіра може підвищити загальний рівень безпеки інформаційних технологій підприємства), спеціальні публікації серії NIST SP 1800-35 (у яких коротко описується, як NCCoE та його співробітники використовують комерційно доступні технології для створення сумісних, заснованих на відкритих стандартах прикладів реалізації ZTA, які відповідають концепціям та принципам, викладеним у NIST SP 800-207), документ Національного центру кібербезпеки Великобританії (NCSC – National Cyber Security Centre) [20] та деякі інші. Далі при викладанні матеріалу скористаємося інформацією та висновками з цих документів, а також з деяких інших публікацій різних міжнародних авторитетних видань, присвячених архітектурі нульової довіри.

Якщо підприємство вирішує прийняти нульову довіру як свою основну стратегію і створити ZTA, розроблену з урахуванням принципів нульової довіри, то воно насамперед зосереджується на суті проблеми, викладеної у визначенні «нульова довіра» [8], яка полягає у тому, щоб запобігти несанкціонованому доступ до даних та послуг/сервісів у поєднанні з максимально детальним контролем доступу. Правила доступу максимально деталізуються, щоб забезпечити мінімальні привілеї, необхідні для виконання дій, зазначених у запиті.

При цьому слід відразу усвідомити (про що говорять багато дослідників), що неможливо створити універсальну архітектуру, принаймні через те, що існують різні підходи до нульової довіри, які залежать від базової архітектури підприємства та вибору, зробленого фахівцями з безпеки. А ось представити набір відповідних компонентів та вимог, які можна використовувати для створення актуальної та ефективної архітектури для конкретного підприємства, це безумовно буде корисним внеском та допомогою у застосуванні тієї чи іншої моделі розгортання ZTA (яких, у принципі, може бути кілька для різних бізнес-процесів на одному підприємстві).

Для початку доречно звернутися до абстрактної моделі доступу з нульовою довірою (рис. 1), представленої в документі NIST [8], та визначити її основні компоненти.

Суб'єктом може бути людина (кінцевий користувач – user) або не фізична сутність (non-person / nonhuman entity) така як пристрій, сервер, сервіс, застосунок тощо [21, 22]. Система може являти собою пристрій, такий як ноутбук, мобільний телефон, віртуальна машина, контейнер тощо. Система покладається на *точку застосування політики* (*policy enforcement point* – PEP), щоб дозволити взаємодію з ресурсом. Суб'єкт взаємодіє із системою, і система має перевірити справжність/ідентифікацію (identity) суб'єкта, а також виконати автентифікацію та авторизацію.

Рис. 1. Абстрактна модель доступу із нульовою довірою

Суб’єкту (користувачу, пристрою, застосунку) потрібен доступ до корпоративного ресурсу. Цей ресурс, що знаходиться під контролем підприємства, може являти собою обчислювальні ресурси, дані, застосунки / сервіси (робоче навантаження), розміщені та керовані локально, у хмарі, на межах або в якійсь їх комбінації [3]. Доступ надається через *точку / пункт прийняття рішення про політику* (*policy decision point* – PDP) і відповідну *точку застосування політики* (PEP). Система з нульовою довірою повинна переконатися, що суб’єкт є справжнім (автентичним), а запит дійсним. PDP/PEP приймає належне рішення, щоб дозволити суб’єкту отримати доступ до ресурсу. Це означає, що нульова довіра стосується двох основних сфер: автентифікації та авторизації. Керування доступом залежить від стану безпеки пристрою (механізму, засобу) та потенційного розгляду інших ситуативних факторів (наприклад, часу та місцезнаходження, попередньої поведінки при доступі тощо), які можуть вплинути на рівень довіри до того, як доступ до ресурсу буде наданий відповідно до певних політик.

Загалом, підприємствам необхідно розробити та підтримувати динамічну політику доступу до ресурсів, що базується на оцінці ризиків, і налаштувати систему, яка гарантуватиме правильне та послідовне застосування цих політик для окремих запитів на доступ до ресурсів. Підприємству не слід покладатися на передбачувану надійність, коли суб’єкт відповідає базовому рівню автентифікації (наприклад, при вході до системи), а усі наступні запити ресурсів вважаються однаково дійсними.

1.1. Основні логічні компоненти архітектури кібербезпеки підприємства, яка базується на принципах нульової довіри

Існує безліч логічних компонентів, з яких може складатися впроваджена на підприємстві ZTA. Ці компоненти можуть працювати як у локальній мережі, так і у хмарі.

Представимо концептуальну архітектуру нульової довіри, яка ґрунтується на ідеї та принципах, викладених у документі NIST [8], одночасно уточнюючи її. Основні логічні компоненти архітектури нульової довіри, а також взаємозв'язок між ними наведено рис. 2.

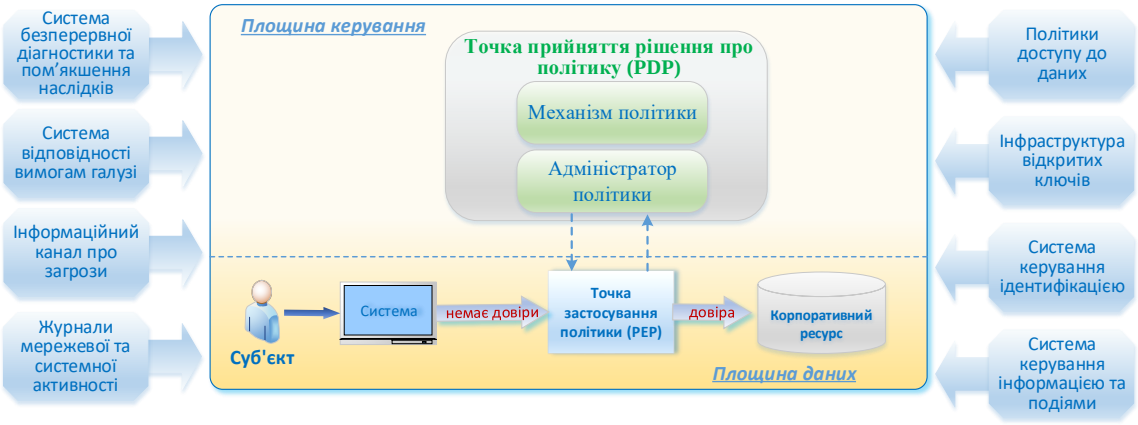

Рис. 2. Основні логічні компоненти архітектури нульової довіри

Передбачається, що суб'єкт функціонує в *недовіреному середовищі* та *недовіреній мережі*, і йому дозволено доступ до *Ресурсу* тільки *через точку застосування політики* (PEP). PEP контролює доступ суб'єкта до ресурсу через те, що NIST називає *зоною неявної довіри* (*implicit trust zone* – представляє собою область, де всі об'єкти є довіреними) [8]. PEP не зберігає і не визначає політику (докладніше призначення PEP розглядається нижче). Цю функцію виконує *точка прийняття рішення про політику* (PDP). Слід також звернути увагу, що *Суб'єкт* взаємодіє з корпоративним ресурсом через так звану *площину даних* (*data plane*), яка відрізняється від *площини керування* (*control plane*), яка використовується логічними компонентами ZTA для зв'язку.

Механізм політики (*policy engine* – PE). Цей компонент відповідає за остаточне рішення щодо надання доступу до ресурсу для даного суб'єкта. PE використовує політику підприємс-

тва, а також вхідні дані із зовнішніх джерел (наприклад, системи безперервної діагностики та пом'якшення наслідків (Continuous Diagnostics and Mitigation – CDM), служби аналізу загроз тощо, які описуються далі) як вхідні дані для алгоритму довіри, щоб надавати, забороняти або скасовувати доступ до ресурсу.

Алгоритм довіри (ТА – *trust algorithm*) – це процес, який використовується РЕ для ухвалення рішення з урахуванням таких вихідних даних, як записи в базі даних політик, роль користувача, відомості про поведінку, інформація про загрози (наприклад, сигнатури атак, що діють в Інтернеті, шкідливі програми тощо) і т. д. відповідно до потреб конкретного розгортання. Кожного разу, коли користувач робить запит на доступ, ТА використовує основну інформацію про ресурс і сторону, що запитує (наприклад, операційну систему (ОС), рівень виправлення / оновлення (patch), використовуваний застосунок). Інформація про користувача, автентифікація, що виконується РЕ, та інші атрибути, такі як час та місцезнаходження, також можуть бути використані ТА для обчислення рівня довіри. Щодо вимог доступу до ресурсу, то сюди можна віднести політики, що ґрунтуються на мінімальних вимогах для доступу, встановлених власником / адміністратором, наприклад, вимога багатофакторної автентифікації з нового місцезнаходження.

Алгоритм довіри може бути реалізований у різний спосіб [8, 23]:

– *ТА на основі критеріїв та оцінок*. ТА на основі критеріїв (Criteria-based ТА) вимагає, щоб сукупність певних атрибутів була обов'язково врахована, перш ніж дозволити виконання певної дії (наприклад, читання/запис). Ці критерії налаштовуються підприємством і мають бути налаштовані окремо для кожного ресурсу. Доступ надається або дія застосовується до ресурсу, лише якщо виконано всі критерії. *ТА на основі оцінок* (*Score-based TA*) обчислює рівень довіри на основі значень для кожного джерела даних і вагових коефіцієнтів, налаштованих підприємством. Якщо оцінка перевищує налаштоване порогове значення для ресурсу, доступ надається або виконується дія. В іншому випадку запит відхиляється або привілеї доступу зменшуються (наприклад, надається доступ для читання, але не для запису до файлу, або повна заборона доступу).

– *Сингулярний* (*Singular*) та *контекстний / контекстуальний* (*Contextual*) ТА. При ухваленні рішень у *сингулярному* ТА не враховується історична інформація користувача, що може прискорити процес ухвалення рішення, але існує ризик того, що деякі атаки можуть залишитись непоміченими, якщо вони залишаються в межах дозволеної ролі користувача (суб'єкта). Навпаки, *контекстуальний ТА* використовує історичні моделі поведінки користувача (суб'єкта) або мережевого агента під час оцінювання запитів на доступ. Це означає, що РЕ повинен підтримувати деяку інформацію про стан усіх суб'єктів і застосунків, але при цьому він може з більшою ймовірністю виявити зловмисника, який використовує підроблені облікові дані для доступу до інформації за шаблоном, який є нетиповим для того, що спостерігає РЕ для даного суб'єкта. Це також означає, що РЕ повинен бути поінформований про поведінку користувача від адміністратора політики (і РЕР), з якими суб'єкти взаємодіють під час комунікації. Аналіз поведінки суб'єкта може бути використаний для створення моделі прийнятного використання, і відхилення від цієї поведінки можуть викликати додаткові перевірки автентифікації або відхилення запитів ресурсів.

Механізм політики працює в парі з іншим компонентом – адміністратором політики (РА). Механізм політики приймає та реєструє рішення (як ухвалене або відхилене), а адміністратор політики виконує це рішення. Як тільки ТА прийняв відповідне рішення, РЕ передає його РА, який налаштовує всі відповідні точки застосування політики, щоб увімкнути або вимкнути з'єднання. Наприклад, він може надіслати налаштування шлюзам та агентам, тим самим вимагаючи повторної автентифікації, повторної авторизації або розриву з'єднання відповідно до певних політик.

Адміністратор політики (*Policy administrator* – РА). Цей компонент відповідає за встановлення та/або відключення шляху зв'язку між суб'єктом і ресурсом (через команди відповідним точкам застосування політики). Він може генерувати будь-які специфічні для сеансу

ідентифікатори та токени автентифікації або облікові дані, що використовуються клієнтом для доступу до корпоративного ресурсу. Він тісно пов'язаний з PE і покладається на його рішення – остаточно дозволити або заборонити сеанс. Якщо сеанс авторизовано, а запит автентифікований, PA налаштовує точку застосування політики (PEP), щоб дозволити розпочати сеанс. Якщо сеанс відхилено (або попереднє схвалення відхилено), PA сигналізує PEP закрити з'єднання. У деяких реалізаціях PE та PA можуть розглядатися як одна служба. В даному випадку вона поділяється на дві логічні складові. PA взаємодіє з PEP під час створення каналу зв'язку. Цей зв'язок здійснюється через площину керування.

Точка застосування політики (*Policy enforcement point* – PEP). Цей компонент відповідає за підключення, моніторинг та завершення з'єднань між суб'єктом та корпоративним ресурсом. PEP зв'язується з PA для надсилання запитів та/або отримання оновлень політики від PA. Це єдиний логічний компонент в архітектурі нульової довіри, але він може бути розбитий на два різні компоненти: клієнт (наприклад, агент на пристрої) та сторона ресурсу (наприклад, компонент шлюзу перед ресурсом, який контролює доступ) або єдиний компонент порталу, що виконує роль сторожа для комунікаційних шляхів. За межами PEP знаходиться довірча зона, де розміщено корпоративний ресурс.

Існує три типи PEP [7]: *PEP агента користувача* (*user agent PEP*), *PEP мережі* та *PEP застосунку*.

PEP мережі вважається найбільш простими з концептуальної точки зору в моделях нульової довіри, оскільки створення мереж нульової довіри зазвичай є найпоширенішою відправною точкою. Мережеві PEP існують у багатьох організаціях. Корпоративні міжмережові екрани (сьогодні це, як правило, брандмауери наступного покоління – NGFW – *Next-Generation Firewalls*) можна розглядати як PEP з нульовою довірою, хоч і з деякими застереженнями. Наприклад, чи можна вважати точкою застосування політики деякий базовий брандмауер п'ятирічної давності? Так, він, звичайно ж, є «точкою контролю мережі» у тому сенсі, що він має правила контролю доступу, які він забезпечує. Однак такий міжмережевий екран навряд чи буде точкою застосування політики (PEP) з нульовою довірою, оскільки він не відповідатиме таким вимогам, як: мати можливість застосовувати модель політики PDP, орієнтовану на ідентифікацію та контекстну залежність; автоматично реагувати на зміни політики, які визначаються PDP; використовувати канал керування для зв'язку з PDP. Адже кожен PEP повинен мати можливість отримувати постійні оновлення від PDP і автоматично коригувати політику, яку він застосовує практично в реальному часі і без втручання людини. Це єдиний спосіб досягти гнучкого та динамічного характеру, властивого підходу нульової довіри, навіть у невеликих масштабах [7].

Оскільки такі точки застосування політики працюють на мережному рівні, вони можуть здійснювати контроль мережного трафіку (як метаданих, так і фактичних даних про трафік), і тому вони є природними точками застосування політики.

PEP застосунків можуть бути зовнішніми по відношенню до застосунків (наприклад, система PAM – *Privileged Access Management* – керування привілейованим доступом) або DLP – *Data Loss Prevention* – запобігання втраті даних) або внутрішніми, наприклад, агент, що працює з *робочим навантаженням* (*workload*). В останньому випадку PEP можна використовувати для локального застосування політик на хості, наприклад, для застосування правил брандмауера локальної ОС. Крім того, точка застосування політики логічно може бути частиною самого застосунку, спираючись на зовнішні атрибути або дії, що впливають на застосунок.

PEP агента користувача – це компоненти, які запускаються на пристрої користувача та надають функції, які часто потрібні для систем з нульовою довірою, такі як встановлення зашифрованого з'єднання через ненадійну мережу. Ці PEP часто використовуються для аналізу пристрою з метою отримання інформації, яка використовується як вхідні дані для політик (наприклад, конфігурації пристрою та стану безпеки). Такий PEP також може взає-

модіяти з суб'єктом (кінцевим користувачем), наприклад, запитуючи додаткову автентифікацію або повідомляючи його.

Слід мати на увазі, що в деяких випадках межа між цими типами точок застосування політики нечітка, і функції, які вони виконують, можуть частково перекриватися. Наприклад, відомо, що IDS/IPS (система виявлення вторгнень / система запобігання вторгненням) можуть бути мережевими або хост-орієнтованими. Аналогічно функції DLP можуть бути реалізовані всередині мережевого пристрою, такого як NGFW, або на хості. В принципі, не так важливо, чи діють конкретні точки застосування політики, такі як DLP та PAM, на мережевому рівні або на рівні застосунків (або на обох). Важливо те, що і DLP, і PAM слід розглядати як частину PEP з нульовою довірою, а їхні політики логічно мають бути частиною моделі нульової довіри. В ідеалі для цього має бути інтеграція між ними та системою нульової довіри. Зрештою, все залежить від конкретної реалізації. Тобто функціональність та поведінка PEP залежатимуть від обраної платформи та від варіанта її розгортання.

Крім цих основних компонентів на підприємстві, що реалізує архітектуру нульової довіри, є ряд зовнішніх компонентів, які сприяють реалізації безпеки з нульовою довірою. А саме існує кілька джерел даних, які надають вхідні дані та правила політик, які використовуються механізмом політик при прийнятті рішень про доступ. До них належать локальні джерела даних, а також зовнішні (тобто не контрольовані або не створені підприємством) джерела даних. Зокрема такі (рис. 2):

– *Система безперервної діагностики та пом'якшення наслідків* (CDM). Вона збирає інформацію про поточний стан корпоративного активу та застосовує оновлення до конфігурації та компонентів програмного забезпечення. Корпоративна система CDM надає механізму політики (PE) інформацію про актив, який надсилає запит на доступ, наприклад, чи працює на ньому відповідна виправлена операційна система, чи забезпечується цілісність дозволених для використання на підприємстві програмних компонентів або присутні недозволені компоненти і чи немає в активу відомих вразливостей. Системи CDM також відповідають за ідентифікацію та потенційне застосування підмножини політик на некорпоративних пристроях, активних в інфраструктурі підприємства.

– *Система відповідності вимогам галузі* (*Industry compliance system*). Гарантується, що підприємство буде відповідати всім нормативним вимогам, під які воно може підпадати (наприклад, вимоги щодо безпеки інформації в галузі охорони здоров'я або фінансової галузі). Сюди входять усі правила політики, які підприємство розробляє задля забезпечення відповідності.

– *Інформаційний(і) канал(и) про загрози (Threat intelligence feed(s)).* Це інформація з внутрішніх або зовнішніх джерел, яка допомагає механізму політики приймати рішення про доступ. Це можуть бути кілька служб, які отримують дані з внутрішніх і/або кількох зовнішніх джерел і надають інформацію про нещодавно виявлені атаки або вразливості, а також нещодавно виявлені недоліки в програмному забезпеченні, нещодавно виявлені шкідливе програмне забезпечення, зареєстровані атаки на інші активи, до яких механізм політики захоче заборонити доступ із корпоративних активів.

– *Журнали мережевої та системної активності (Network and system activity logs).* Ця корпоративна система об'єднує журнали активів, мережевий трафік, дії з доступу до ресурсів та інші події, які дозволяють в режимі реального часу (або майже реального часу) отримувати інформацію про стан безпеки корпоративних інформаційних систем.

– *Політики доступу до даних (Data access policies).* Це атрибути, правила та політики доступу до ресурсів підприємства. Цей набір правил може бути закодований (через інтерфейс керування) або динамічно згенерований механізмом політик. Ці політики є відправною точкою авторизації доступу до ресурсу, оскільки вони надають основні привілеї доступу для облікових записів і застосунків / сервісів на підприємстві. Ці політики мають ґрунтуватися на певних цільових ролях та потребах організації.

– *Інфраструктура відкритих ключів підприємства (Public Key Infrastructure – PKI).* Ця система відповідає за створення та реєстрацію сертифікатів, виданих підприємством ресурсам, суб'єктам, службам та застосункам. Вона також включає глобальну екосистему центрів сертифікації та національну PKI, яка може бути інтегрована або не інтегрована із корпоративною PKI. Це також може бути PKI, що не базується на сертифікатах X.509.

– *Система керування ідентифікацією (ID management system).* Вона відповідає за створення, зберігання та керування обліковими записами корпоративних користувачів та ідентифікаційними записами (наприклад, сервер полегшеного протоколу доступу до каталогів – LDAP). Ця система містить необхідну інформацію/дані про суб'єкт (наприклад, ім'я, адресу електронної пошти, сертифікати) та інші характеристики, такі як роль, атрибути доступу та призначені активи підприємства. Вона часто використовує інші системи (наприклад, PKI) для артефактів (об'єктів), пов'язаних з обліковими записами користувачів. Крім того вона може бути частиною більшої об'єднаної спільноти і може включати некорпоративних співробітників або посилання на некорпоративні активи для спільної роботи.

– *Система керування інформацією та подіями безпеки* (*SIEM* – це область комп'ютерної безпеки, в якій програмні продукти та послуги поєднують у собі управління інформацією про безпеку (*SIM – security information management*) та управління подіями безпеки (*SEM – security event management*)). Тут збирається інформація, пов'язана з безпекою, для подальшого аналізу. Ці дані потім використовуються для уточнення політик та попередження про можливі атаки на активи підприємства.

Усі перелічені вище логічні компоненти не обов'язково повинні бути унікальними системами. Один актив може виконувати функції кількох логічних компонентів, і так само логічний компонент може складатися з кількох апаратних або програмних елементів для виконання завдань. Наприклад, інфраструктура відкритих ключів, керована підприємством, може складатися з одного компонента, що відповідає за видачу сертифікатів для пристроїв, та іншого компонента, що використовується для видачі сертифікатів кінцевим користувачам, але обидва використовують проміжні сертифікати, видані одним і тим самим корпоративним кореневим центром сертифікації підприємства. У деяких продуктах, що підтримують концепцію нульової довіри та представлені сьогодні на ринку, компоненти PE і PA об'єднані в одну службу.

1.2. Підходи до реалізації архітектури нульової довіри

На думку фахівців NIST, архітектура нульової довіри може різнитися залежно від потреб компанії. Для цього вони розглядають можливість застосування кількох різних підходів (шляхів), за допомогою яких підприємство може запровадити ZTA для робочих процесів, зокрема: *вдосконалене/покращене управління ідентифікацією* (*enhanced identity governance*), *логічну мікросегментацію* (*logical micro-segmentation*) та *сегментацію на основі мережі* (*network-based segmentation*) [8]. Ці підходи відрізняються компонентами, що використовуються, і основним джерелом правил політики для організації. При цьому слід зазначити, що одні підходи найбільше підходять для одних випадків, тоді як інші доцільно використовувати в інших ситуаціях. Тому підприємство, яке прагне розробити ZTA, може виявити, що обраний ним варіант використання та існуючі політики виділяють один підхід серед інших існуючих. Однак це не означає, що інші підходи не працюватимуть. Зважаючи на все, це лише вказує на те (і не більше), що інші підходи можуть бути більш важкими для реалізації і можуть вимагати кардинальніших змін в організації розвитку бізнесу.

Архітектура нульової довіри з вдосконаленим управлінням ідентифікацією

Підхід до розробки архітектури нульової довіри, що ґрунтується на *вдосконаленому управлінні ідентифікацією*, використовує ідентичність (*identity*) учасників як ключовий компонент створення політики. У рамках цього підходу політики доступу до ресурсів підприємства ґрунтуються на ідентифікації та встановлених атрибутах. Основна вимога для отримання доступу до ресурсів базується на привілеях доступу, наданих даному суб'єкту.

Інші фактори, такі як використовуваний пристрій, стан активів і фактори середовища, можуть змінити остаточний результат визначення рівня довіри (і остаточний дозвіл на доступ) або будь-яким чином скоригувати результат, наприклад, надати тільки частковий доступ до заданого джерела даних в залежності від розташування в мережі. Окремі ресурси або компоненти PEP, що захищають ресурс, повинні мати можливість перенаправляти запити до служби механізму політики або автентифікувати суб'єкт і схвалити запит перед наданням доступу. Підходи, що ґрунтуються на вдосконаленому управлінні ідентифікацією, для підприємств часто застосовуються з використанням моделі відкритої мережі або корпоративної мережі з доступом сторонніх користувачів («гостей») або частою присутністю в мережі пристроїв, що не належать підприємству (некорпоративних пристроїв). Спочатку доступ до мережі надається всім активам, але доступ до корпоративних ресурсів обмежується обліковими записами з відповідними привілеями доступу. При цьому надання базових можливостей підключення до мережі має також і недолік: зловмисники все одно можуть спробувати провести розвідку мережі та/або використовувати її для атак типу «відмова в обслуговуванні» як усередині компанії, так і проти третьої сторони. Підприємствам, як і раніше, необхідно відстежувати таку поведінку та реагувати на неї перш, ніж вона вплине на робочі процеси.

Архітектура нульової довіри з використанням мікросегментації

Підприємство може вибрати реалізацію архітектури нульової довіри, що базується на розміщенні окремих ресурсів або груп ресурсів в унікальному сегменті мережі, захищеному компонентом безпеки шлюзу. У цьому підході підприємство розміщує інфраструктурні пристрої, такі як інтелектуальні комутатори (або маршрутизатори) або міжмережеві екрани наступного покоління або спеціальні шлюзи, які діють як PEP, захищаючи кожен ресурс або невелику групу пов’язаних ресурсів. Як альтернатива (або додатково) підприємство може вибрати мікросегментацію на основі хоста за допомогою програмних агентів або брандмауерів на активі(ах) кінцевої точки. Ці шлюзові пристрої динамічно надають доступ до окремих запитів від клієнта, активу або сервісу. Залежно від моделі, шлюз може бути єдиним компонентом PEP або частиною багатокомпонентного PEP, що складається зі шлюзу та агента на стороні клієнта. Для повноцінного функціонування цього підходу потрібна програма/система управління ідентифікацією (identity governance program – IGP), але при цьому передбачається, що компоненти шлюзу будуть виступати в ролі PEP, що захищає ресурси від несанкціонованого доступу та/або виявлення. Ключова необхідність цього підходу полягає в тому, щоб компоненти PEP керувалися та мали можливість реагувати та змінювати конфігурацію за потреби для відповіді на загрози або зміни в робочому процесі. Можна реалізувати деякі функції мікросегментованого підприємства за допомогою менш просунутих шлюзів і навіть міжмережевих екранів без збереження стану, але витрати на адміністрування та труднощі швидкої адаптації до змін роблять такий вибір вкрай небажаним.

Архітектура нульової довіри з використанням мережевої інфраструктури та програмно визначених периметрів

Даний підхід використовує мережеву інфраструктуру для реалізації архітектури нульової довіри. Реалізація архітектури нульової довіри може бути досягнута за допомогою оверлейної мережі (overlay network). Подібні підходи іноді називають підходами програмно визначеного периметра (*software defined perimeter* – SDP) [24, 25] і часто включають концепції програмно визначених мереж (*Software Defined Networks* – SDN) [26] і мереж IBN (intent-based networking – іноді перекладаються як мережа на основі намірів, інтенційно-орієнтована мережа) [27]. У цьому підході адміністратор політики виступає у ролі мережевого контролера, який налаштовує та реконфігурує мережу на основі рішень, прийнятих механізмом політики. Клієнти продовжують запитувати доступ через точки застосування політики, якими керує компонент PA. Коли підхід реалізується на мережевому рівні застосунків (тобто на рівні 7 моделі OSI – *Open Systems Interconnection*), найпоширенішою моделлю розгортання є модель розгортання на основі агента пристрою/шлюзу (яка буде розглянута далі). У цій реалізації агент і шлюз ресурсу (діють як єдиний PEP та налаштовані PA) встановлюють за-

хищений канал, що використовується для зв'язку між клієнтом та ресурсом. Можливі інші варіанти цієї моделі, наприклад, для хмарних віртуальних мереж, мереж, не заснованих на IP-протоколах тощо.

З іншого боку, доцільним є розгляд потенційних рішень з нульовою довірою з погляду їх моделей розгортання, які можуть бути корисною основою, за допомогою якої підприємства зможуть оцінити потенційних постачальників відповідних рішень, аналізуючи їх плюси та мінуси. Вважається, що багато з корпоративних моделей нульової довіри, що надаються постачальниками, будуть відповідати одній або декільком моделям розгортання. Такі моделі дозволяють оцінити, як насправді можуть бути розгорнуті системи з нульовою довірою, хоча, звичайно ж, реальна архітектура розгортання залежатиме від можливостей обраної технології.

Існує кілька варіантів розгортання вибраних компонентів архітектури. Залежно від того як налаштовано корпоративну мережу для різних бізнес-процесів на одному підприємстві можуть використовуватися кілька моделей розгортання архітектури нульової довіри. Розглянемо деякі відомі моделі розгортання нульової довіри.

1.3. Моделі розгортання нульової довіри

Насамперед, слід звернути увагу на те, що для простоти (зручності) подальшого викладу матеріалу на всіх рисунках, наведених далі та асоційованих з відповідними моделями розгортання, будуть опущені пов'язані з PDP системи (такі як: CDM, система відповідності вимогам галузі, система керування ідентифікацією тощо), які були представлені раніше на рис. 2. Хоча реально всі ці зв'язки PDP з відповідними логічними компонентами архітектури нульової довіри, як і раніше, залишаються актуальними і присутні незалежно від того, яка модель розгортання з нульовою довірою буде обрана та використовуватися для конкретної реалізації.

Модель розгортання на основі агента пристрою/шлюзу

Модель агента пристрою/шлюзу (*Device Agent/Gateway Model*; іноді цю модель називають моделлю розгортання на основі ресурсів – *resource-based deployment model* [7]) представлена на рис. 3.

Рис. 3. Модель розгортання на основі агента пристрою/шлюзу

У даній моделі розгортання зазвичай у системі суб'єкта є розгорнутий користувальницький агент, що діє як PEP агента користувача. Крім того, існує вбудований PEP (шлюз), який розгортається (відповідно до бачення NIST [8]) на ресурсі або у вигляді компонента безпосередньо перед ресурсом. Наприклад, на кожному корпоративному активі, наданому підприємством, встановлений агент пристрою, який координує з'єднання, а на кожному ресурсі є компонент (шлюз), який розміщується безпосередньо перед ресурсом, так що ресурс взаємодіє тільки зі шлюзом (по суті, виступаючи як проксі для ресурсу). Агент направляє частину або весь потік даних на відповідний PEP обробки запитів. Шлюз відповідає за взаємодію з адміністратором політики та дозволяє лише узгоджені комунікаційні шляхи, налаштовані PA. Наприклад, у типовій ситуації суб'єкт із ноутбуком (як деяким активом виданим підприємст-

вом) хоче підключитися до корпоративного ресурсу (наприклад, до застосунку/бази даних відділу кадрів). Запит на доступ приймається локальним агентом, який потім перенаправляється адміністратору політики. Адміністратор політики та механізм політики можуть бути локальним ресурсом підприємства або хмарною службою. Адміністратор політики передає запит до механізму політики для аналізу. Якщо запит авторизований, адміністратор політики настроює канал зв'язку між агентом пристрою та відповідним шлюзом ресурсів через площину керування. Для цього може використовуватися така інформація, як адреса інтернет-протоколу (IP), інформація про порт, ключ сеансу та інші параметри безпеки. Після чого агент пристрою та шлюз з'єднуються, і починається передача зашифрованих потоків даних застосунків/служб. З'єднання між агентом пристрою та шлюзом ресурсів переривається або після завершення робочого процесу, або з ініціативи адміністратора політики – через порушення безпеки (наприклад, закінчення часу очікування сеансу, неможливості повторної автентифікації тощо). Цю модель доцільніше використовувати для підприємств, які мають ефективну систему керування пристроями, а також окремі ресурси, які можуть взаємодіяти зі шлюзом [8]. Наприклад, для підприємств, які активно використовують хмарні сервіси, – це клієнт-серверна реалізація програмно-визначуваного периметра (SDP) альянсу з безпеки хмарних обчислень (*Cloud Security Alliance* – CSA) [28, 29]. Ця модель також підходить для підприємств, які не хочуть вводити політику BYOD (оскільки в ній доступ можливий лише через агента пристрою, розміщеного на активах, що належать підприємству).

Як зазначається у роботі [7], дана модель має такі переваги: комплексний (наскрізний – end-to-end) контроль доступу до застосунків та мережевого трафіку; дуже компактна неявна зона довіри, яка знаходиться за шлюзом.

У цій же роботі вказується й на недоліки, притаманні цій моделі, зокрема:

– необхідність розгортання PEP як на пристроях, так і на ресурсах;

– існує ймовірність технічних конфліктів між компонентами ресурсів та PEP;

– PEP повинні бути доступні для розгортання на різних, можливо, застарілих / успадкованих ОС;

– існує ймовірність негативного відношення (сприйняття) з боку власників ресурсів застосунків (власники можуть не захотіти розгортати будь-яке додаткове програмне забезпечення у своїх комерційних або критично важливих для бізнесу застосунках);

– потрібні зв'язки один до одного: між PEP і ресурсами (тобто ця модель вимагає розгортання одного PEP для кожного керованого ресурсу, що може накласти значне функціональне навантаження (навантаження з керування) на систему нульової довіри і команду (робочу групу), що відповідає за неї;

– наскрізний захищений тунель може перешкоджати (заважати) нормальному функціонуванню існуючих вбудованих засобів контролю безпеки. У багатьох системах нульової довіри мережевий трафік від PEP агента користувача до PEP ресурсу шифрується. Це безпечно та ефективно, але зазвичай має побічний ефект, який полягає в тому, що весь цей трафік стає непрозорим для будь-якого посередника. Це вигідно, якщо посередником є зловмисник, але шкідливо, якщо це, наприклад, розгорнутий на підприємстві компонент безпеки, такий як мережева IDS/IPS;

– PEP має бути видимим та доступним віддаленим користувачам. Насправді для розгортання систем з нульовою довірою відповідно до цієї моделі буде потрібна окрема можливість безпечного віддаленого доступу – в ідеальному випадку як частина платформи нульової довіри. Зазвичай комерційні платформи з нульовою довірою вирішують це завдання за допомогою комбінації периферійного PEP і відповідного PEP агента користувача.

Модель розгортання з мікросегментацією

Дана модель розгортання (micro-segmentation deployment model) орієнтована на варіант використання між серверами («сервер-сервер») [7]. Ця модель дозволяє підійти до проблеми з точки зору ресурсів, а не користувачів. Ресурси вважаються основними суб'єктами (нефізичними особами/сутностями – non-person entities – NPE), щодо яких мають бути розроблені та

застосовані політики (рис. 4). Дана модель по суті є варіантом попередньої розглянутої моделі (моделі, що базується на ресурсах, – моделі розгортання на основі агента пристрою/шлюзу). Важливою її відмінністю від попередньої моделі є те, що ресурси насправді є суб'єктами (автентифікованими ідентифікаторами).

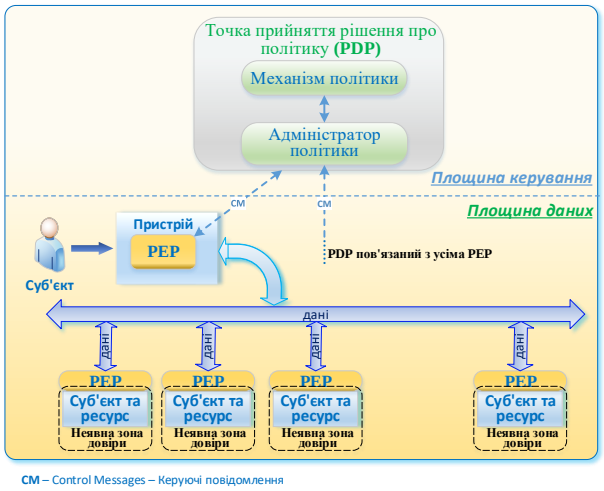

Рис. 4. Модель розгортання із мікросегментацією

Як правило, суб'єкти NPE матимуть більш слабкі форми ідентифікації, ніж люди, а саме, здебільшого на основі сертифікатів і, швидше за все, на основі одного фактора автентифікації. Найчастіше цей сертифікат генерується та керується центром сертифікації підприємства.

Переваги використання цієї моделі [7]: невелика неявна зона довіри (зазвичай обмежена лише самим ресурсом); точний, двонаправлений контроль доступу до ресурсів (для серверів або мікросервісів). Оскільки PEP виконується локально по відношенню до ресурсу, його політики можуть контролювати як вихідні, так і вхідні мережеві з'єднання (ці політики можна застосовувати як до ресурсів на рівні сервера, так і до мікросервісів).

До недоліків цієї моделі можна віднести [7]: необхідність розгортання PEP як на пристроях користувача, так і на ресурсах; наявність ймовірності технічних конфліктів між компонентами ресурсів та PEP; PEP повинні бути доступні для розгортання на множині, можливо, застарілих або успадкованих ОС; наявність можливого негативного відношення з боку власників ресурсів; необхідні взаємозв'язки один до одного між PEP та ресурсами; може не найкращим чином підходити для доступу користувачів до ресурсів; відсутність віддаленого доступу (не передбачено) – потрібний прямий доступ суб'єктів до PEP. Крім того, не слід забувати про потенційний недолік, зумовлений функціональними або архітектурними вадами (недоліками), пов'язаними з реалізацією сценарію «користувач–сервіс» конкретним постачальником або у відкритому вихідному коді.

Модель розгортання на основі анклаву

Ця модель розгортання є також різновидом розглянутої вище моделі агента пристрою/шлюзу. У цій моделі компоненти шлюзу (PEP) знаходяться перед кількома ресурсами, які називаються анклавом ресурсів (resource enclave). Цей набір ресурсів може бути фізично розташований разом (наприклад, у локальному або суміщеному центрі обробки даних) або логічно пов'язаний (наприклад, набір серверів хмари). Як і в попередній моделі, суб'єкт має додатковий локально встановлений PEP агента користувача (рис. 5).

Рис. 5. Модель розгортання на основі анклаву

Важливо розуміти, що у цій моделі неявна зона довіри містить кілька мережевих ресурсів, які, швидше за все, взаємодіють між собою. Тобто дуже важливо, щоб у цій моделі анклав ресурсів працював виключно у логічній приватній мережі, яка перебуває під контролем підприємства. Хоча ресурси всередині анклаву здатні і можуть взаємодіяти один з одним за межами видимості та контролю PEP, єдиний спосіб для суб'єктів поза зоною довіри – взаємодіяти з ним через PEP (який повинен знаходитись під контролем політики). Тобто, використовуючи цю модель, підприємствам необхідно ретельно вивчити дані ресурсів та моделі взаємодії.

Ця модель в цілому простіше в розгортанні, ніж попередня – модель агента пристрою/шлюзу, оскільки в ній задіяно на порядок менше PEP завдяки зв'язку «один до багатьох» між PEP та ресурсами. А відсутність необхідності розгортання додаткового програмного забезпечення на ресурсах не лише спрощує роботу, а й дозволяє уникнути більшості технічних або конфліктів політик із застосунками та їх власниками. Перевага цього рішення полягає також у тому, що PEP розгортаються на межі корпоративної мережі (у DMZ – Demilitarized Zone – демілітаризована зона), тому вони можуть бути природною точкою входу для віддалених користувачів. Зрозуміло, вони також служитимуть точкою застосування політики для локальних користувачів, чий трафік залишиться повністю всередині підприємства. Ідея полягає в тому, щоб PEP могли реагувати на зміни в ресурсах, що захищаються, наприклад, виявляючи поява нових ресурсів і використовуючи атрибути ресурсів (метадані) для застосування до них політик.

Ця модель корисна для підприємств із застарілими / успадкованими (legacy) застосунками або локальними центрами обробки даних, у яких неможливо встановити окремі шлюзи (для встановлення / налаштування агентів пристроїв підприємству необхідна надійна програма (система) управління активами та конфігурацією). Також організації, які працюють у нових середовищах (особливо на базі IaaS – Infrastructure-as-a-Service) або використовують програмно-керовану інфраструктуру (наприклад, DevOps – development and operations), добре підходять для цієї моделі. Організаціям з нижчим рівнем операційної зрілості, меншою прозорістю або складними успадкованими мережами може знадобитися розгорнути більше PEP, щоб зменшити розмір та масштаб кожної неявної зони довіри. Як альтернативу, вони можуть використовувати гібридний підхід, який підтримують деякі постачальники архітектури нульової довіри, поєднуючи цю модель з моделлю мікросегментації.

Недоліком моделі розгортання на основі анклаву є те, що шлюз (PEP) захищає колекцію ресурсів і може бути не в змозі захистити кожен ресурс окремо. Це також може дозволити суб'єктам бачити ресурси, до яких вони не мають прав доступу.

Модель розгортання з використанням хмарної маршрутизації

У наступній моделі (рис. 6), що одержала назву моделі розгортання з використанням хмарної маршрутизації (cloud-routed), весь трафік від суб'єкта проходить через хмарне середовище, перш ніж досягти ресурсу. Ця модель є досить поширеним підходом, який використовується багатьма комерційними виробниками [7].

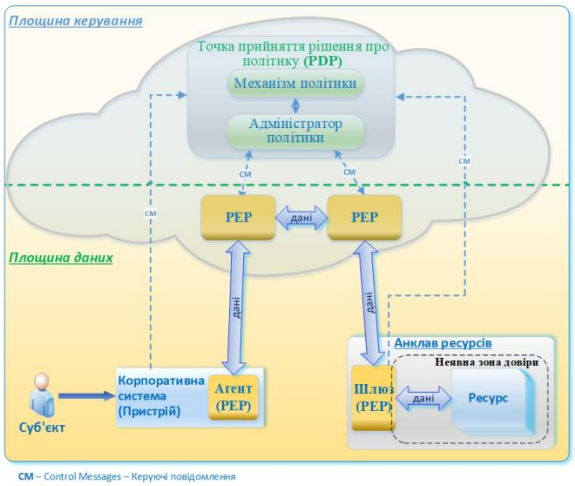

Рис. 6. Модель розгортання з використанням хмарної маршрутизації

Як видно з рис. 6, у цій моделі PEP, що знаходяться перед анклавами ресурсів підприємства, діють аналогічно до PEP (шлюзу) у моделі, показаній вище (рис. 5). Однак у цих PEP є одна важлива відмінність – вони не є точкою входу до корпоративної мережі. Замість цього дана функціональність була логічно перекладена на PEP, розташовані в хмарному середовищі постачальника. У цій моделі PEP, розташовані лише на рівні підприємства (локальні – on-premises), виступають у ролі сполучних ланок, забезпечуючи вихідні з'єднання з хмарним PEP. Оскільки ці внутрішньокорпоративні конектори не вимагають будь-яких вхідних з'єднань, вони часто спрощують розгортання цієї моделі в обмін на деякі обмеження. Коли суб'єкт хоче зв'язатися з ресурсом, він спочатку проходить автентифікацію в PDP, а потім його потік даних спрямовується на один з хмарних PEP, зазвичай, той, який розташований найближче до нього (або має найменшу затримку). Потім відповідний потік даних проходить через PEP у хмарі до PEP, який має з'єднання з цільовим анклавом ресурсів. Локальний (розташований на підприємстві) PEP забезпечує безпеку анклаву ресурсів так само, як і у моделі розгортання на основі анклаву (рис. 5).

Як зазначається у роботі [7], дана модель має певні переваги та недоліки (табл. 1).

Таблиця 1

Переваги та недоліки моделі розгортання з використанням хмарної маршрутизації

Переваги	Недоліки
✓ Більш просте налаштування для підприємств. ✓ Платформа «як послуга» (As-a-Service) знижує операційні витрати підприємства. ✓ Постачальники, які використовують цю модель, також для захисту доступу до загальнодоступних веб-сайтів надають послугу SWG (Secure Web Gateway – безпечний / захищений веб-шлюз).	✓ PEP можуть бути розгорнуті без належного контролю за безпекою, мережею та дотриманням нормативних вимог. ✓ Збільшує затримку трафіку користувача і потенційно знижує пропускну здатність. ✓ Підтримує лише обмежену кількість мережевих протоколів. ✓ Не підходить для локальних користувачів, які отримують доступ до локальних ресурсів. ✓ Потенційно велика, непрозора або шумна неявна зона довіри.

Модель розгортання на основі порталу ресурсів

У цій моделі розгортання (рис. 7) точка застосування політики (PEP) є окремим компонентом, що виконує роль шлюзу для запитів суб'єктів. Портал-шлюз може бути призначений для окремого ресурсу або безпечного анклаву для сукупності ресурсів, що використовуються для виконання однієї бізнес-функції. Як приклад можна навести портал-шлюз у приватній хмарі або центрі обробки даних, що містить успадковані застосунки.

Основна перевага цієї моделі перед іншими полягає в тому, що програмний компонент (PEP) не потрібно встановлювати на всі пристрої клієнта. До того ж, ця модель гнучкіша для політики BYOD та проєктів спільної роботи між організаціями.

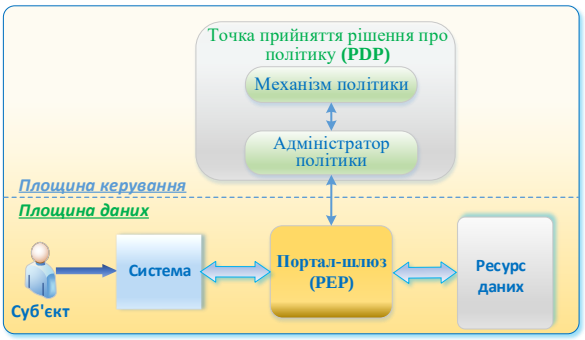

Рис. 7. Модель розгортання на основі порталу ресурсів

Корпоративні адміністратори не повинні стежити за тим, щоб на кожному пристрої перед використанням було встановлено відповідний локальний агент – агент пристрою (PEP агента користувача). Хоча від пристроїв, які вимагають доступ, можна отримати певну інформацію. Крім того, у цій моделі сканування та аналіз активів та пристроїв може здійснюватися тільки після їх підключення до порталу PEP, а постійний моніторинг щодо наявності шкідливих програм, невиправлених вразливостей та відповідної конфігурації може бути неможливим. А оскільки локальний агент, який обробляє запити, відсутній, то на корпоративному рівні може не бути повної прозорості або можливості здійснювати довільний контроль над активами (оскільки їх можна побачити / просканувати лише при підключенні до порталу). Хоча для пом'якшення або компенсації наслідків на підприємстві можуть застосовуватися такі заходи, як ізоляція браузера (browser isolation – це модель кібербезпеки, метою якої є фізична ізоляція активності/дій користувачів Інтернету (і пов'язаних з ними кіберризиків) від їх локальних мереж та інфраструктури).

Як недолік слід зазначити, що використання цього рішення також дозволяє зловмисникам виявляти портал і використовувати його для доступу до нього з метою проведення атаки на кшталт «відмова в обслуговуванні» (DoS – denial-of-service). У зв'язку з чим системи порталу повинні мати достатні ресурси, щоб забезпечити доступність при DoS-атаках або збоях у роботі мережі.

Модель розгортання на основі використання «пісочниці» застосунків

Ще один варіант моделі розгортання на основі агента пристрою/шлюзу полягає в тому, що перевірені / схвалені застосунки або процеси запускаються на активах в ізольованих середовищах/системах (пісочниці – sandboxing). Ці системи можуть бути віртуальними машинами, контейнерами, модулями довіреної платформи та іншими реалізаціями. Вони мають одну мету – захистити застосунок або екземпляри застосунків від можливо скомпрометованого хоста або інших застосунків, що працюють на цьому активі / хості [8]. На рис. 8 пристрій суб'єкта запускає попередньо узгоджені та перевірені застосунки у «пісочниці».

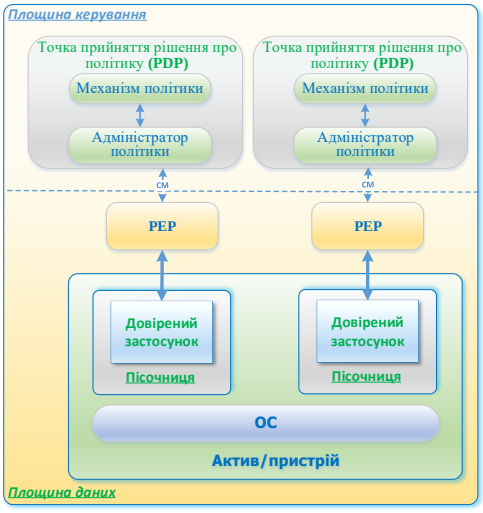

Рис. 8. Модель розгортання на основі використання «пісочниці» застосунків

Застосунки можуть взаємодіяти з PEP для запиту доступу до ресурсів, але PEP відхилятиме запити від інших застосунків активу. Ця модель PEP може бути локальною службою підприємства або хмарною службою.

Основна перевага цього варіанта моделі полягає в тому, що деякі застосунки відокремлені від решти активу. Якщо актив не може бути просканований на предмет вразливостей, ці окремі застосунки, поміщені в «пісочницю» (так звані ізольовані застосунки), можуть бути захищені від потенційного зараження шкідливим програмним забезпеченням (ПЗ) на хості активу.

Одним із недоліків цієї моделі є те, що підприємства повинні підтримувати ці ізольовані застосунки для всіх активів і можуть не мати повної видимості клієнтських активів. Крім того, підприємству необхідно переконатися в безпеці кожного ізольованого застосунку, що може вимагати більше зусиль, ніж простий моніторинг пристроїв.

Таким чином, очевидно, що всі розглянуті моделі можуть дати новий рівень деталізації того, як насправді можуть бути розгорнуті системи з нульовою довірою. Хоча при цьому не слід забувати, що реальна архітектура розгортання, звичайно ж, залежатиме від можливостей обраної технології. Також було б некоректним під час розгляду парадигми нульової довіри не відзначити можливість існування певних ризиків, пов'язаних із використанням архітектури нульової довіри.

1.4. Загрози, пов’язані з архітектурою нульової довіри

Як відомо, жодне підприємство не може усунути ризик кібербезпеки [8]. І це, незважаючи на належно реалізовані та підтримувані архітектурою нульової довіри вказівки щодо кібербезпеки, управління ідентифікацією та доступом, безперервним моніторингом та загальною кібергігієною, що дозволяють зменшити загальний ризик та захистити від поширених загроз. Причому деякі загрози мають унікальні особливості під час впровадження архітектури нульової довіри. Тому далі розглянемо найбільш відомі загрози, пов’язані з архітектурою нульової довіри, та деякі рекомендації щодо їх усунення.

Спотворення процесу прийняття рішень у рамках архітектури нульової довіри

В архітектурі нульової довіри механізм політики (PE) та адміністратор політики (PA) є ключовими компонентами всього підприємства. Жодної взаємодії між ресурсами підприємства не відбувається, якщо вона не схвалена і, можливо, не налаштована механізмом політики та адміністратором політики. Це означає, що ці компоненти необхідно правильно налаштувати, постійно контролювати (будь-які зміни конфігурації повинні реєструватися та підлягати аудиту) та підтримувати у відповідному стані. В іншому випадку будь-який адміністратор підприємства, який має доступ до конфігурації правил PE, може внести несхвалені зміни або зробити помилку, яка може порушити роботу підприємства, або скомпрометований PA може дозволити доступ до ресурсів, які в інших випадках (наприклад, до зламаного особистого пристрою) не були б схвалені.

Відмова в обслуговуванні або порушення роботи мережі

Як було зазначено вище, в архітектурі нульової довіри адміністратор політики є ключовим компонентом забезпечення доступу до ресурсів, тому ресурси підприємства не можуть підключатись один до одного без дозволу PA і, можливо, без дій щодо налаштування. Якщо зловмисник порушує або забороняє доступ до PEP або PE/PA (тобто DoS-атака або захоплення каналу), це може негативно вплинути на роботу підприємства. Підприємства можуть знизити цю загрозу, розташувавши механізм застосування політик у належно захищеному хмарному середовищі або реплікувавши її в кількох місцях відповідно до рекомендацій щодо забезпечення кіберстійкості [30]. Це зменшує ризик, але не усуває його. Наприклад, ботнети, подібні до Mirai (це сімейство шкідливих програм, схожих на хробаків, які заражали IoT-пристрої та об'єднували їх у DDoS-ботнет) [31–33] здійснюють масовані DoS-атаки на основних інтернет-провайдерів і порушують роботу мільйонів інтернет-користувачів. Також існує ймовірність того, що зловмисник може перехопити та заблокувати трафік до PEP або

PA для частини або всіх облікових записів користувачів на підприємстві. Наприклад, у філії або навіть в одного віддаленого співробітника (у таких випадках страждає лише частина суб'єктів підприємства). Хоча, насправді, таке можливе і у застарілих VPN з віддаленим доступом і не є унікальним тільки для архітектури нульової довіри. З іншого боку хостинг-провайдер може випадково перевести хмарний механізм політики або адміністратора політики в режим offline. У цьому випадку механізм політики або компонент адміністратора політики стане недоступним із мережі. І як результат – через неполадки в роботі, може припинитися робота всього підприємства. Крім того, існує також ризик, що ресурси підприємства можуть бути недоступні для адміністратора політики, тому навіть якщо суб'єкту буде надано доступ, адміністратор політики не зможе налаштувати канал обміну даними через мережу. Це може статися в результаті DDoS-атаки або просто через надмірну інтенсивність використання, що раптово виникла. Все це аналогічно до будь-якого іншого порушення роботи мережі, коли деякі або всі суб'єкти підприємства не можуть отримати доступ до певного ресурсу, оскільки він з якоїсь причини недоступний.

Крадіжка облікових даних

Відомо, що розроблена та реалізована архітектура нульової довіри повинна перешкоджати доступу скомпрометованого облікового запису або активу до ресурсів. З іншого боку, правильно реалізовані політики нульової довіри, інформаційної безпеки та стійкості до відмов, а також кращі практики знижують ризик отримання зловмисником широкого доступу до ресурсів підприємства через вкрадені облікові дані або інсайдерську атаку. Тому, виходячи зі всього сказаного, з великою часткою ймовірності, можна припустити, що основною метою для зловмисників будуть відповідні облікові записи з політиками доступу до ресурсів. Оскільки зловмисникам, щоб впровадитись на підприємство, необхідно скомпрометувати існуючий обліковий запис або пристрій. З цією метою зловмисники можуть використовувати фішинг, соціальну інженерію або комбінацію атак, щоб отримати повноваження важливих облікових записів. При цьому застосування MFA (multi-factor authentication – багатофакторна автентифікація) для обробки запитів на доступ може знизити ризик втрати інформації внаслідок компрометації облікового запису. Однак зловмисник з валідними обліковими даними (або зловмисник-інсайдер) все одно зможе отримати доступ до ресурсів, до яких цьому обліковому запису вже було надано права доступу. Наприклад, зловмисник або скомпрометований співробітник, який має облікові дані та активи дійсного співробітника відділу кадрів, що належать підприємству, все одно зможе отримати доступ до бази даних працівників.

У свою чергу, використання архітектури нульової довіри все ж таки дозволяє знизити ризик і запобігати бічному переміщенню будь-яких скомпрометованих облікових записів або активів по мережі. Якщо скомпрометовані облікові дані не авторизовані для доступу до певного ресурсу, їм, як і раніше, буде відмовлено у доступі до цього ресурсу. Крім того, контекстний алгоритм довіри з більшою ймовірністю виявить цю атаку і швидко відреагує на неї, ніж при атаці в застарілій (успадкованій) мережі, що базується на периметрі. Контекстний алгоритм довіри може виявити шаблони доступу, які виходять за рамки звичайної поведінки, та заборонити скомпрометованому обліковому запису або внутрішній загрозі доступ до конфіденційних (чутливих, важливих, критичних – sensitive) ресурсів.

Видимість у мережі

Для виявлення та реагування на потенційні атаки на ресурси підприємства весь трафік у мережі має перевірятися, реєструватися та аналізуватись [8]. Однак частина трафіку в мережі підприємства може бути непрозорою для засобів мережевого аналізу на рівні 3 (мережевому рівні) моделі OSI. Цей трафік може походити від активів, що не належать підприємству (наприклад, від сторонніх служб, які використовують інфраструктуру підприємства для доступу до Інтернету), або від застосунків / сервісів, які не піддаються пасивному моніторингу. Тому підприємство, яке не може виконати ретельну перевірку пакетів або вивчити зашифрований трафік – змушене використовувати інші методи для оцінки можливої присутності зловмисника у мережі. Наприклад, на підприємстві можна збирати метадані (адреси джерела

та призначення тощо) про зашифрований трафік і використовувати їх для виявлення активного зловмисника або можливого шкідливого ПЗ, що працює в мережі. Крім того, для аналізу трафіку, який неможливо розшифрувати та вивчити, можна використовувати методи машинного навчання. Зокрема, автори роботи [34], проаналізувавши шість поширених алгоритмів машинного навчання, показали, як кожен із них вирішує проблему виявлення шкідливих зашифрованих мережевих сеансів. Тому використання машинного навчання потенційно дозволяє підприємству класифікувати трафік як дійсний або, навпаки, шкідливий та той що потребує ліквідації наслідків.

Зберігання системної та мережевої інформації

Наступна загроза для корпоративного моніторингу та аналізу мережного трафіку – це сам компонент аналізу. Якщо результати сканування монітора, мережевий трафік та метадані зберігаються для побудови контекстних політик, проведення експертизи або подальшого аналізу, ці дані стають об'єктом атаки зловмисників. Подібно до мережевих діаграм, конфігураційних файлів та інших документів мережевої архітектури, ці ресурси повинні бути захищені. Якщо зловмиснику вдасться отримати доступ до цієї інформації, він зможе отримати уявлення про архітектуру підприємства та визначити активи для подальшої розвідувальної діяльності та атак.

Ще одним джерелом інформації для зловмисника на підприємстві з нульовою довірою є інструмент керування, який використовується для кодування політик доступу. Як і трафік, що зберігається, цей компонент містить політики доступу до ресурсів і може дати зловмиснику інформацію про те, які облікові записи найбільш цінні для компрометації (наприклад, ті, які мають доступ до ресурсів даних, що цікавлять зловмисника). Що стосується всіх важливих корпоративних даних, то для запобігання несанкціонованому доступу та спробам доступу до них також необхідно забезпечити належний захист. Оскільки ці ресурси є критично важливими для безпеки, вони повинні мати найсуворіші політики доступу та бути доступними лише зі встановлених або спеціальних облікових записів адміністраторів.

Залежність від пропрієтарних форматів даних або рішень

При прийнятті рішень про доступ архітектура нульової довіри спирається на кілька різних джерел даних, включаючи інформацію про запитуючого суб'єкта, використовувані активи, корпоративні та зовнішні джерела інформації, а також дані із аналізу існуючих загроз. Найчастіше активи, що використовуються для зберігання та обробки цієї інформації, не мають загального, відкритого стандарту взаємодії та обміну інформацією. Це може призвести до того, що через проблеми із сумісністю підприємство буде прив'язане до певного кола постачальників. Якщо у одного з постачальників виникають проблеми з безпекою або збої в роботі, підприємство не зможе перейти до нового постачальника без значних витрат (наприклад, заміни кількох активів) або тривалої процедури перетворень (наприклад, перетворення правил політики з одного пропрієтарного формату на інший). Тому щоб знизити пов'язані з цим ризики, підприємствам слід оцінювати постачальників послуг комплексно, враховуючи такі фактори, як контроль безпеки постачальника, витрати підприємства на його переоснащення та управління ризиками в ланцюжку поставок, безумовно, на додаток до більш характерних показників, таких як продуктивність, стабільність тощо.

Використання сутностей, які не є фізичними особами, при адмініструванні архітектури нульової довіри

Зважаючи на те, що штучний інтелект та інші програмні агенти все частіше використовуються для управління безпекою в корпоративних мережах, вони (як відповідні компоненти) повинні взаємодіяти з компонентами управління архітектури нульової довіри (наприклад, механізмом політики, адміністратором політики), причому іноді замість людини-адміністратора. Однак питання про те, як ці компоненти проходять автентифікацію на підприємстві, що запроваджує ZTA, залишається відкритим.

У більшості автоматизованих інформаційних систем передбачається, що при використанні програмного інтерфейсу застосунку (API – application programming interface) для

доступу до компонентів ресурсів використовуватимуться ті чи інші засоби автентифікації. Пов'язаний із цим ризик полягає в тому, що зловмисник зможе спонукати або змусити NPE виконати якесь завдання, на виконання якого він не має привілеїв. Програмний агент може мати більш низькі вимоги до автентифікації (наприклад, ключ API порівняно з MFA) для виконання адміністративних завдань або завдань, пов'язаних із безпекою, порівняно з людиною-користувачем. Якщо зловмисник може взаємодіяти з агентом, він теоретично може обманом змусити агента надати йому ширший доступ або виконати якесь завдання від імені зловмисника. Існує також ризик, що зловмисник може отримати доступ до облікових даних програмного агента та видати себе за нього під час виконання завдань.

При цьому слід мати на увазі, що найбільший ризик при використанні автоматизованих технологій для конфігурування та застосування політик – це можливість помилкових спрацьовувань (нешкідливі дії, прийняті за атаки) та помилкових заперечень (атаки, прийняті за нормальну діяльність), що впливають на рівень безпеки підприємства. Зменшити цей ризик можна за допомогою регулярного проведення додаткового аналізу для виправлення помилкових рішень та покращення процесу прийняття рішень.

Таким чином, можна зробити висновок, що реалізація архітектури нульової довіри – це досить складний процес, причому це швидше за все шлях (рух), ніж повна заміна інфраструктури або технологічних процесів. Організація повинна прагнути до поступового впровадження принципів нульової довіри, змін у процесах та технологічних рішень, які захищають її найцінніші активи даних. Більшість підприємств, швидше за все, продовжуватимуть працювати у комбінованому режимі з використанням нульової довіри та периметра протягом невизначеного періоду часу, продовжуючи вкладати кошти у постійну модернізацію IT [8]. При цьому наявність плану модернізації IT, що включає перехід до архітектури, яка базується на принципах ZT, може допомогти підприємству сформувати дорожні карти для здійснення невеликих переходів на нові робочі процеси. Зрештою, те, як підприємство переходитиме на цю концепцію, залежатиме від його поточного стану кібербезпеки та операційної діяльності. Причому підприємство має досягти базового рівня підготовленості (базовий рівень включає визначення та класифікацію активів, суб'єктів, бізнес-процесів, потоків даних і відображення залежностей для підприємства), перш ніж стане можливим розгорнути масштабну систему, орієнтовану на нульову довіру. Підприємству необхідна ця інформація, щоб визначити список бізнес-процесів-кандидатів та суб'єктів/активів, які будуть залучені до цього процесу. При цьому, найбільшою проблемою, що перешкоджає впровадженню успішних рішень в області нульової довіри, на думку фахівців ACT-IAC (American Council for Technology-Industry Advisory Council – Американська рада з технологій – Консультативна рада з питань промисловості), може бути загальний недостатній рівень кібербезпеки [35]. Ними зазначається, наприклад, що більшість державних установ не мають фундаментальних основ (таких як, політик, процесів та інструментів), необхідних для розгортання систем, що відповідають концепції нульової довіри.

В цілому ж, основними перевагами впровадження концепції нульової довіри, у тому числі виділеними авторами робіт [21, 36], можна вважати такі:

– Поліпшення видимості мережі, виявлення порушень та керування вразливостями (покращення видимості того, які користувачі, коли, як і звідки отримують доступ до тих чи інших ресурсів).

– Перешкода поширенню шкідливих програм (більш ефективне виявлення, реагування та відновлення після інцидентів, що дозволяє мінімізувати наслідки витоків; мінімізація ризику бокового переміщення).

– Скорочення капітальних та експлуатаційних витрат на безпеку.

– Скорочення обсягу та вартості робіт із забезпечення відповідності нормативним вимогам.

– Усунення необхідності пошуку винних (наприклад, при деяких інцидентах мережева команда може звинуватити службу безпеки у зриві робіт, а служба безпеки може звинуватити

мережеву команду; Zero Trust намагається змусити технологічні підрозділи подолати відповідні протиріччя між різними робочими групами).

– Підвищення обізнаності та розуміння даних.

– Захист ресурсів та активів (запобігання витоку важливих даних до зловмисників (обмеження кількості зломів (витоків) за рахунок зниження можливостей зловмисників); зменшення внутрішньої загрози; захист важливих (sensitive) корпоративних даних за допомогою надійного шифрування як під час їх передачі, так і у стані спокою; виконання динамічної оцінки доступу до ресурсів з урахуванням ризиків шляхом безперервної переоцінки всіх операцій та сеансів доступу, збору інформації, отриманої в результаті періодичної повторної автентифікації та повторної авторизації, постійної перевірки стану пристрою, аналізу поведінки, постійної перевірки стану ресурсів, виявлення аномалій та інших аналітичних даних щодо безпеки).

– Забезпечення цифрової трансформації бізнесу (підтримка віддаленої роботи; надання працездатних пристроїв від постачальників; підвищення якості обслуговування кінцевих користувачів).

2. Рекомендації щодо успішного впровадження архітектури нульової довіри

Спираючись на досвід впровадження систем нульової довіри відомими у світі організаціями та компаніями, викладений у різних авторитетних міжнародних виданнях [7, 8, 21], сформулюємо деякі рекомендації для успішного впровадження архітектури нульової довіри на типовому IT-підприємстві у вигляді послідовності певних кроків/етапів. При цьому доречно відразу ж звернути увагу (знову ж таки, виходячи з досвіду впровадження) на те, що керівництво IT-підприємства має прагнути до поступового впровадження принципів нульової довіри, зміни процесів та технологічних рішень, що захищають його найцінніші активи даних. Такий поступовий підхід дозволить знизити ризик відмов і помилок у системі, допоможе зрозуміти подальші процеси розгортання елементів системи, а також полегшить перехід персоналу до нової архітектури.

Перш ніж розпочинати впровадження архітектуру нульової довіри на підприємстві, необхідно провести дослідження активів, суб'єктів, потоків даних та робочих процесів, оскільки підприємство не в змозі визначити, які нові процеси або системи необхідно запровадити, якщо немає уявлення про поточний стан операційної діяльності. Крім того, щоб підприємство «нульової довіри» могло успішно функціонувати, механізм політики повинен мати знання про суб'єктів підприємства. Суб'єкти можуть включати як людей, так і можливі нефізичні особи/сутності, такі як облікові записи сервісів, які взаємодіють із ресурсами. На рис. 9 подано процес поетапного впровадження архітектури нульової довіри на IT-підприємстві.

Рис. 9. Процес поетапного впровадження архітектури нульової довіри

Етап 1. *Виявлення та інвентаризація активів підприємства*. Перший крок, який мають зробити відповідні співробітники підприємства на шляху до «нульової довіри», – це ідентифікувати всі свої активи, визначивши, які ресурси є в існуючому середовищі (обладнання, програмне забезпечення, застосунки, дані та сервіси). Для цього може знадобитися розгортання інструментів для моніторингу трафіку з метою виявлення активних ресурсів, які використовуються та до яких здійснюється доступ. Необхідно

мати повне уявлення про ресурси підприємства (як локальних, так і хмарних) та провести їх облік (визначити їхню кількість, розташування, поточну захищеність, їх важливість та вплив на роботу підприємства), оскільки це саме ті об'єкти, для захисту яких буде розроблено архітектуру нульової довіри. Крім того, передбачається необхідність ідентифікації та моніторингу пристроїв, що не належать підприємству, які можуть перебувати в мережній інфраструктурі, що належить підприємству, або мати доступ до корпоративних ресурсів. Після створення чіткого списку ресурсів, необхідно визначити їх стан: чи потребують вони заміни на більш нові пристрої та чи мають користувачі проблеми із доступом до них на даний момент. Якщо ресурси не враховані, то, швидше за все, вони не будуть належним чином захищені в рамках архітектури нульової довіри. Вони можуть бути вразливими для витоку, модифікації, видалення, відмови в обслуговуванні або інших типів атак.

Етап 2. *Розробка політик доступу для підтримки завдань та корпоративних сценаріїв використання*. Після того, як співробітниками підприємства будуть визначені всі ресурси, які потрібно захистити, та місце їх розташування, необхідно сформулювати політики, які будуть застосовуватись у рамках архітектури нульової довіри, щоб визначити, кому та за яких умов дозволено доступ до кожного ресурсу. Політики доступу повинні бути розроблені таким чином, щоб дозволи та повноваження на доступ до кожного ресурсу відповідали принципам найменших привілеїв та поділу обов'язків. Це вимагає розуміння категорій користувачів, які отримуватимуть доступ до ресурсів, їх вимог до доступу, місць роботи, умов контракту, типів пристроїв та моделей власності (наприклад, BYOD, корпоративна), оскільки все це впливатиме на створення політики. Дозволи на доступ можуть бути обмежені залежно від місцезнаходження особи, яка запитує доступ, часу доби або інших параметрів, які можуть додатково обмежувати доступ без втручання у роботу підприємства. Усі політики доступу повинні ґрунтуватися на важливості ресурсу, що захищається. У тому числі, враховуючи особливості впровадження багаторівневих політик для архітектури нульової довіри в середовищах застосунків Cloud Native (Cloud Native – це програмний підхід до створення, розгортання та управління сучасними застосунками у середовищах хмарних обчислень [37]), описаних у роботі [38]. При цьому слід враховувати, що підприємства під час розробки політик можуть зіткнутися з певними проблемами. Одна з яких полягає в тому, що архітектура нульової довіри підприємства може складатися з багатьох компонентів, кожен з яких може виконувати функції механізму політики та адміністратора політики. В результаті політика доступу не може бути централізована в одному місці. Правила можуть бути розподілені між численними компонентами, наприклад: деякі правила можуть бути задані в компоненті захисту кінцевих точок, деякі – в компонентах керування ідентифікацією, обліковими даними та доступом, інші правила – у компоненті мережевої безпеки, а треті – у компоненті захисту даних або інших компонентах. Відсутність єдиного місця, де могли б централізовано зберігатись усі правила політики, може ускладнити для підприємства підтримку організованого, повного та послідовного розуміння політики доступу. Щоб допомогти підприємствам керувати політикою доступу, необхідно чітко відстежувати не лише правила доступу, а й те, де кожне з них визначене.

Етап 3. *Визначення існуючих можливостей та технологій забезпечення безпеки*. Якщо підприємство планує впровадити архітектуру нульової довіри у нове середовище, тобто у нього немає існуючого IT-оснащення чи засобів безпеки, які воно хотіло б використати або пристосувати, цей етап не потрібен. Проте більшість підприємств, які впроваджують систему нульової довіри, не починатимуть із нуля. Для них важлива існуюча інфраструктура та технологічні системи, які вже виконують функції безпеки. Як правило, підприємства мають як мінімум мережеві брандмауери та системи виявлення вторгнень для забезпечення безпеки периметра, а також системи керування ідентифікацією та доступом до облікових даних, які дозволяють їм автентифікувати користувачів та забезпечувати авторизований доступ на основі ідентифікаційних даних та ролей. На їх ноутбуках та/або мобільних пристроях можуть бути встановлені системи захисту кінцевих точок, що виконують функції брандмау-

ера та забезпечують роботу необхідного антивірусного або іншого програмного забезпечення. Вони можуть мати інструментальні засоби для управління вразливістю та конфігураціями, ведення журналів та інших функцій, пов'язаних з безпекою. Крім того, вони, швидше за все, мають свого роду центр управління безпекою.

Підприємство повинне визначити та скласти опис існуючих компонентів та можливостей технології безпеки, щоб зрозуміти, які засоби захисту вони вже забезпечують, а потім визначити, чи повинні ці компоненти продовжувати забезпечувати захист у межах розгорнутої архітектури нульової довіри чи їх слід модифікувати (замінити). Щоб заощадити гроші, підприємство буде прагнути продовжувати використовувати або модернізувати якомога більше існуючих технологій, не жертвуючи при цьому безпекою. Продовження використання існуючих технологій вимагатиме від підприємства розуміння того, з якими потенційними компонентами та продуктами нульової довіри буде інтегрована існуюча технологія безпеки. Будь-які додаткові компоненти, які придбаються спеціально для розгортання в рамках ZTA, в ідеалі повинні інтегруватися з компонентами технології безпеки, які організація вже має та планує продовжувати використовувати.

Етап 4. *Усунення недоліків у політиках та процесах забезпечення нульової довіри шляхом застосування підходу, заснованого на оцінці ризиків та цінності даних*. Після того, як співробітники підприємства складуть перелік ресурсів, які необхідно захистити, та наявні можливості щодо забезпечення безпеки, можна приступати до планування відповідної технології захисту доступу, визначаючи, чи буде інфраструктура сегментована і на якому рівні захищатиметься кожен ресурс. Технологія доступу має бути розроблена з використанням підходу, що ґрунтується на оцінці ризику, при якому критично важливі ресурси ізолюються у власних зонах довіри, захищених точками застосування політики, але при цьому допускається спільне використання кількох менш важливих ресурсів в одній зоні довіри. Для успішного захисту ІТ-підприємства треба визначити ризики та надати їм рівні. Рівень небезпечності ризику визначається за допомогою розуміння ймовірності його появи та збитків, які принесе підприємству його реалізація. Після документування ризиків буде зрозуміло, які ресурси є найбільш критично важливими для роботи підприємства та які вразливості вони мають. Ці дії можна порівняти з діями у межах системи керування ризиками (RMF – *Risk Management Framework* [39]), оскільки будь-яке впровадження архітектури нульової довіри – це процес зниження ризику для бізнес-функцій підприємства.

При розробці технології захисту доступу організація повинна визначити, яка точка застосування політики відповідає за захист кожного ресурсу, а також які допоміжні технології братимуть участь у ухваленні рішень щодо доступу до ресурсів. Спочатку мережа підприємства може бути зовсім не сегментована. Фактично до впровадження нульової довіри, коли підприємство все ще покладається на захист на основі периметра, таку технологію можна представити як захист усіх ресурсів підприємства за допомогою однієї точки застосування політики, тобто брандмауером на периметрі. У міру впровадження ZTA підприємство повинне сегментувати свою інфраструктуру на дрібніші частини. Така сегментація дозволить йому обмежити потенційний вплив порушень або атак та полегшить моніторинг мережевого трафіку. Під час розробки системи захисту доступу підприємство повинне застосовувати контроль доступу на кількох рівнях, а саме, на рівні застосунків, вузлів та мережі.

Етап 5. *Впровадження компонентів архітектури нульової довіри та поступове використання існуючих безпекових рішень для досягнення кінцевої мети*. Як тільки на підприємстві буде: а) правильне розуміння існуючого оточення з погляду ресурсів, які необхідно захистити, та вже розгорнутих засобів безпеки; б) сформульовані політики доступу, які підходять для підтримки його завдань та бізнес-показників; в) розроблено технологію захисту доступу із зазначенням рівня деталізації, з яким захищатиметься доступ до різних ресурсів, та допоміжних технологій, які будуть використовуватись у точці прийняття рішення про політику (PDP), підприємство може безпосередньо розпочинати поступове впровадження архітектури нульової довіри.

Як було вказано вище, наразі вже існує декілька моделей розгортання нульової довіри, які є доступними для встановлення на підприємстві. Тому важливо зрозуміти конкретні потреби ІТ-підприємства для визначення придатної для нього архітектури. Так, при визначенні придатного для ІТ-підприємства рішення при застосуванні міжмережевих екранів із точкою прийняття рішень про політику необхідно виходити з функціональних ролей брандмауерів, як елементів інфраструктури – шлюзів (PEP), які беруть участь у детальних мережевих політиках та політиках рівня ідентифікації, у забезпеченні безпеки. NIST, наприклад, визначає наступні типи шлюзів [38]:

– *Вхідний шлюз* (*Ingress gateway*). Цей шлюз керує тим, як застосунки в кластері/групі виходять за його/її межі (наприклад, керує тим, які імена, сертифікати, порти, протоколи та кінцеві точки застосунків обслуговуються за межами кластера).

– *Вихідний шлюз* / *шлюз виходу* (*Egress gateway*). Керує взаємодією програм у кластері/групі із зовнішнім світом. Він може використовуватися для традиційної фільтрації та реєстрації вихідних повідомлень, як проксі Squid, але також може реалізовувати політику на основі ідентифікації для того, що дозволено викликати та виконувати обмін обліковими даними або надавати набір облікових даних від імені програми, щоб програмі не потрібно було їх обробляти.

– *Граничний / крайовий шлюз* (*Edge gateway*). Цей шлюз знаходиться на межі між мережею та вхідним шлюзом. Він приймає зовнішній потік / трафік перед вхідним шлюзом та виконує тонке балансування навантаження між групами або вузлами. Використовується для переривання зовнішнього трафіку, забезпечення стійкості до відмови на рівні інфраструктури, розгортання «синьо-зелених» (blue-green) груп і спрощення розгортання вхідного шлюзу для кожної групи користувачів, не вимагаючи від кожної з цих груп наявності вхідних шлюзів, що публічно маршрутизуються. Синьо-зелене або канаркове (canary) розгортання – це методологія, що дозволяє впровадити удосконалення програми для невеликої підмножини кінцевих користувачів, і якщо все йде добре, поступово збільшувати це співвідношення, поки всі користувачі не перейдуть на нове розгортання [40].

– *Sidecar gateway*. Особливість цього шлюзу полягає у його розташуванні поряд з кожним екземпляром застосунку для перехоплення всього трафіку, що входить і виходить із застосунку, та обробки внутрішніх комунікацій між сервісами в інфраструктурі.

Ідентифікація, автентифікація та авторизація мають вирішальне значення для прийняття рішень щодо доступу до ресурсів. Враховуючи, що ухвалення та виконання рішень про доступ – це дві основні сфери відповідальності ZTA, підприємство захоче використовувати існуюче або нове рішення ICAM (*Identity, Credential, Access Management – керування ідентифікацією, обліковими даними та доступом*) як фундаментальний компонент для початкової реалізації архітектури нульової довіри.

Підприємству слід уважно розглянути можливість запровадження багатофакторної автентифікації для всіх користувачів. Захист кінцевих точок або аналогічне рішення, що може оцінювати стан пристрою та інтегрується з рішенням ICAM, також може стати ще одним основним компонентом початкового розгортання ZTA. Початкова архітектура нульової довіри, що базується на цих основних компонентах, зможе використовувати ідентифікацію та авторизацію суб'єктів, а також стан і відповідність вимогам кінцевих пристроїв, що запитують, як основу для прийняття рішень про доступ. Потім можуть бути розгорнуті додаткові допоміжні компоненти та функції для задоволення більшої кількості вимог ZTA. Які типи компонентів та в якому порядку будуть розгорнуті, залежить від завдань підприємства та конкретних умов використання. Якщо важлива безпека даних, пріоритетними будуть компоненти безпеки даних. Якщо важливо виявлення аномалій з урахуванням поведінки, можна встановити моніторинг і систему аналізу на основі штучного інтелекту (AI – *artificial intelligence*). Архітектуру нульової довіри доцільно будувати поступово, додаючи та інтегруючи все більше допоміжних компонентів, функцій та можливостей, щоб крок за кроком перетворити її на більш повнофункціональну.

При цьому слід розуміти, що при розгортанні рішень, що задовольняють концепцію нульової довіри, може виникнути проблема, пов'язана з так званим людським фактором. На жаль, керівники служб безпеки на деяких підприємствах стикаються із протидією змінам із боку деяких осіб. Це може бути обумовлено культурою, технічними упередженнями або емоційною орієнтацією на існуючі інструменти або архітектуру безпеки [7]. Ця проблема може здаватися незначною у порівнянні з фінансовими та апаратними складовими, однак це може викликати серйозні проблеми із впровадженням. Є кілька способів протистояти цьому. Насамперед, це навчання (підвищення рівня обізнаності, кваліфікації). Тому дуже важливо належним чином підійти до питання створення майбутніх користувачів архітектури нульової довіри. Успіх впровадження архітектури нульової довіри багато в чому залежатиме від знання основних принципів нульової довіри, які застосовуються до ситуації, а також методів, необхідних для забезпечення дотримання цих принципів. У узагальненому вигляді дана інформація міститься у табл. 2 [23].

Таблиця 2

Принципи (основи) нульової довіри, завдання та методи, пов'язані з реалізацією принципів

Принципи (основи)	**Ціль (завдання)**	**Методи реалізації принципу**
Ресурси.	Ідентифікація та класифікація ресурсів (попередня умова для всіх інших принципів).	Керування ідентифікацією (користувачі, пристрої).
Усі комунікаційні зв'язки захищені незалежно від розташування мережі.	Застосування однієї і тієї ж політики безпеки для внутрішніх та зовнішніх запитів доступу.	Сегментація (сегментація мережі та застосунків для застосування політик ближче до даних або ресурсів), автентифікація та авторизація всіх запитів як внутрішніх, так і зовнішніх, шифрування всіх комунікацій як внутрішніх, так і зовнішніх.
Доступ до ресурсів надається на основі кожного з'єднання.	Права доступу до попереднього з'єднання або сеансу не впливають на права наступного сеансу; доступ суворо обмежений ресурсом, що запитується.	Автентифікація сеансів, детальний контроль доступу на рівні ресурсів.
Доступ до ресурсів надається на основі динамічних політик, які враховують стан ідентифікації користувача/пристрою та можуть включати інші поведінкові атрибути.	Необхідно реалізувати динамічні політики доступу, які враховують стан ідентифікатора користувача, стан пристрою користувача та його атрибути поведінки.	Автентифікація та авторизація на основі контексту, ризик-орієнтована (розрахунок оцінки ризику на основі контексту та історії), адаптивні та динамічні методи контролю доступу.
Усі належні ресурси/пристрої знаходяться у найбільш безпечному стані.	Постійна діагностика та пом'якшення наслідків для оцінки стану пристрою; скомпрометовані пристрої повинні бути позбавлені доступу.	Моніторинг стану пристрою, зв'язку. Автентифікація на основі поведінки для заборони доступу до скомпрометованих пристроїв.
Усі автентифікації та авторизації ресурсів є динамічними та підлягають неухильному виконанню.	Автентифікація та авторизація є безперервними та автоматичними процесами, що переглядають та адаптують довіру до нових та поточних комунікацій.	Безперервна автентифікація та авторизація, адаптивні політики доступу, повторна автентифікація та повторна авторизація, автоматизація автентифікації та авторизації.
Збір інформації для коригування та підвищення рівня безпеки.	Безперервний збір даних для виявлення загроз у системі з автоматичним застосуванням необхідних заходів безпеки.	Реєстрація дій, моніторинг мережі, виявлення та аналіз загроз; оперативна реконфігурація.

Етап 6. *Перевірка реалізації для підтвердження підсумкових досягнень під час розгортання архітектури нульової довіри*. Вибрані для тестування сценарії використання повинні відповідати тим, які найбільше точно відображають повсякденний доступ користувачів

підприємства до його ресурсів. В ідеалі підприємство може створити набір тестів, які можна використовувати для перевірки можливостей у рамках ZTA не лише перед розгортанням кожної нової можливості в процесі поступового розгортання архітектури нульової довіри, а й на основі регулярного тестування, коли розгортання ZTA вважається завершеним. Наприклад, проведення тестування на проникнення та можливості викрадення даних, протистояння фішинговим атакам, фальсифікації тощо.

Етап 7. *Постійне вдосконалення та розвиток відповідно до змін характеру загроз, завдань, технологій та нормативних документів*. Після того як архітектура нульової довіри буде розгорнута і буде вважатися завершеною, вона повинна продовжувати адаптуватися до умов, що змінюються. Якщо технологічні компоненти, що використовуються в ZTA, модернізуються або застарівають, їх слід замінити. Якщо з'являються нові інноваційні технології, підприємство повинне розглянути можливість їх інтеграції в існуючу архітектуру нульової довіри, щоб скористатися перевагами нових засобів захисту, методів та механізмів, які можуть підвищити рівень безпеки підприємства. Якщо цілі підприємства в сфері безпеки змінюються, або внаслідок зміни завдань, або внаслідок змін у нормативних документах, може знадобитися зміна політик та самої архітектури нульової довіри, щоб найкраще відповідати цим новим цілям. Тобто в рамках цього безперервного процесу валідації та вдосконалення підприємства повинні постійно контролювати свою мережу та іншу інфраструктуру, а також оновлювати політики, технології та топології сегментації мережі, щоб переконатися, що вони залишаються ефективними.

Наприкінці хочеться, по перше, ще раз відзначити, що розгортання та впровадження архітектури нульової довіри – це складний, тривалий, багатоетапний і безперервний процес, який передбачає виконання кропіткої роботи для досягнення якісніших рішень у забезпеченні безпеки ІТ-підприємства. По-друге, зупинитися на існуючих сьогодні проблемах і тенденціях, пов'язаних із розвитком та впровадженням архітектури нульової довіри на підприємствах. А саме, сьогодні, в принципі, визначено основи архітектур нульової довіри, але як зробити так, щоб різні технології відповідали вимогам до архітектури нульової довіри, як і раніше, залишається непростим завданням [41]. В даний час контроль доступу, автентифікація особистості та оцінка довіри в архітектурі нульової довіри все ще знаходяться на стадії дослідження, тому питання про те, як використовувати зазначені напрацювання для підвищення рівня захисту безпеки та практичного застосування архітектури нульової довіри, залишається актуальною темою, яка заслуговує на окремий розгляд.

Тим не менш, існуючі вже сьогодні рішення побудови систем на основі архітектур нульової довіри та досвід їх використання свідчать про істотні переваги нової концепції перед традиційними архітектурами, орієнтованими на захист по периметру. А матеріал, представлений у цій роботі, на нашу думку, допоможе відповідним спеціалістам розібратися з фундаментальними змінами у підході до інформаційної безпеки, кібербезпеки та використати відповідні рекомендації щодо успішного впровадження архітектури нульової довіри на своїх ІТ-підприємствах.

Висновки

1. Архітектура нульової довіри – це план кібербезпеки підприємства, який використовує концепції нульової довіри та охоплює зв’язки компонентів, планування робочого процесу та політики доступу. А її реалізація – це шлях, який потрібно пройти, а не просто повна заміна інфраструктури або технологічних процесів.

2. Модель розгортання на основі агента пристрою/шлюзу доцільніше використовувати для підприємств, які мають ефективну систему управління пристроями, а також окремі ресурси, які можуть взаємодіяти зі шлюзом. Ця модель також підходить для підприємств, які не хочуть запроваджувати політику BYOD.

3. Модель розгортання з мікросегментацією орієнтована на варіант використання між серверами. Переваги використання даної моделі полягають у невеликій неявній зоні довіри

та точному двонаправленому контролі доступу до ресурсів (для серверів або мікросервісів). Серед недоліків даної моделі можна виділити: необхідність розгортання точок застосування політики як на пристроях, так і на ресурсах; наявність ймовірності технічних конфліктів між компонентами ресурсів та PEP; точки застосування політики повинні бути доступні для розгортання на множині, можливо, застарілих або успадкованих ОС; наявність можливих негативних відносин з боку власників ресурсів застосунків; необхідність взаємозв'язків один до одного між PEP та ресурсами; може не підходити для доступу користувачів до ресурсів; потрібний прямий доступ суб'єктів до точок застосування політики.

4. Модель розгортання на основі анклаву є корисною для підприємств із успадкованими застосунками або локальними центрами обробки даних, у яких неможливо встановити окремі шлюзи. Також цю модель доречно використовувати організаціям, які працюють у нових середовищах (особливо на базі IaaS) або використовують програмно-керовану інфраструктуру. Недоліком цієї моделі розгортання є те, що шлюз захищає колекцію ресурсів і може бути не в змозі захистити кожен ресурс окремо. Це може дозволити суб'єктам бачити ресурси, до яких вони не мають прав доступу.

5. Модель розгортання з використанням хмарної маршрутизації більш проста та зручна в установці система для підприємств. Проте слід пам'ятати, що простота розгортання не може бути виправданням використання недостатньо ефективного механізму управління безпекою. Дана модель зазвичай добре підходить тільки для віддалених користувачів, оскільки весь трафік повинен проходити через хмару постачальника, а якщо користувачі знаходяться в локальній мережі і отримують доступ до локальних ресурсів, їх дані недоцільно переправляти через хмару постачальника, так як це збільшує затримки, знижує пропускну здатність та збільшує витрати підприємства.

6. Основною перевагою моделі розгортання на основі порталу ресурсів перед іншими моделями є те, що програмний компонент (PEP) не потрібно встановлювати на усі клієнтські пристрої. До того ж, ця модель гнучкіша для політики BYOD та проєктів спільної роботи між організаціями. Як недолік слід зазначити, що використання цього рішення може дозволити зловмисникам виявляти портал та використовувати його для доступу до нього з метою проведення атаки на кшталт «відмова в обслуговуванні». У зв'язку з чим системи порталу повинні мати достатні ресурси, щоб забезпечити доступність при DoS-атаках або збоях у роботі мережі.

7. Основна перевага моделі розгортання на основі використання «пісочниці» застосунків полягає в тому, що певні програми відокремлені від решти активу. При цьому одним із недоліків цієї моделі є те, що підприємства повинні підтримувати такі ізольовані застосунки для всіх активів і можуть не мати повної видимості клієнтських активів. Крім того, підприємству необхідно переконатися в безпеці кожного ізольованого застосунку, що може вимагати більше зусиль, ніж простий моніторинг пристроїв.

8. Говорячи про можливість і доцільність застосування тієї чи іншої моделі розгортання з нульовою довірою, слід відзначити те, що на одному підприємстві для різних бізнес-процесів можуть використовуватися кілька моделей розгортання ZTA, все залежатиме від того, як організована корпоративна мережа на конкретному підприємстві.

9. Під час впровадження архітектури нульової довіри можуть виникати деякі специфічні загрози, які мають унікальні особливості (наприклад, спотворення процесу прийняття рішень у рамках архітектури нульової довіри; відмова в обслуговуванні або порушення роботи мережі; крадіжка облікових даних (інсайдерська загроза); видимість у мережі; зберігання системної та мережевої інформації; залежність від пропрієтарних / власних форматів даних або рішень; використання сутностей, які не є фізичними особами при адмініструванні ZTA), для яких також мають місце певні рішення у межах реалізації певної ZTA.

10. Представлені дослідження покликані допомогти спеціалістам з безпеки розібратися в новій парадигмі забезпечення кібербезпеки інформаційних систем сучасних цифрових

підприємств та використати надані рекомендації щодо успішного впровадження архітектури нульової довіри на своїх IT-підприємствах.

Список літератури:

1. Buck C., Olenberger C., Schweizer A., Völter F., Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust // Computers & Security. 2021. 110. 102436.
2. Trend Micro Incorporated. What Is Zero Trust? URL: https://www.trendmicro.com/en_us/what-is/what-is-zero-trust.html. (дата звернення: 10.07.2024).
3. Kerman A., Borchert O., Rose S., Division E., Tan A. Implementing a zero trust architecture // National Institute of Standards and Technology, 2020. 17 p. URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf. (дата звернення: 10.07.2024).
4. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture. (дата звернення: 10.07.2024).
5. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Огляд існуючих моделей та основних принципів нульової довіри // Радіотехніка. 2024. Вип. 217. С. 39–54.
6. Fernandez E. B., Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA) // Computer Standards & Interfaces. 2024. Vol. 89. 103832. https://doi.org/10.1016/j.csi.2024.103832.
7. Garbis J., Chapman J. W. Zero Trust Security: An Enterprise Guide. Berkeley, CA: Apress, 2021. 300 p.
8. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. https://doi.org/10.6028/NIST.SP.800-207.
9. Saltzer J. H., Schroeder M. D. The protection of information in computer systems // Proceedings of the IEEE. 1975. 63(9). P. 1278–1308.
10. Shapiro J. S., Hardy N. EROS: A principle-driven operating system from the ground up // IEEE software. 2002. 19(1). P. 26–33.
11. Bishop M. Introduction to computer security. Addison-Wesley Professional. 2004. 747 p.
12. Samaniego M., Deters R. Zero-trust hierarchical management in IoT // 2018 IEEE international congress on Internet of Things (ICIOT). IEEE, 2018. P. 88–95.
13. Teerakanok S., Uehara T., Inomata A. Migrating to zero trust architecture: Reviews and challenges // Security and Communication Networks. 2021. 2021(1). 9947347. https://doi.org/10.1155/2021/9947347.
14. Adahman Z., Malik A. W., Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security // Computers & Security. 2022. Vol. 122. 102911. https://doi.org/10.1016/j.cose.2022.102911
15. Fortinet. The State of Zero Trust. Report. 2023. URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-zero-trust.pdf. (дата звернення: 10.07.2024).
16. Martinez J. Zero Trust Architecture: 2024 Complete Guide. URL: https://www.strongdm.com/zero-trust. (дата звернення: 10.07.2024).
17. Shore M., Zeadally S., Keshariya A. Zero trust: the what, how, why, and when // Computer. 2021. 54(11). P. 26–35. https://doi.org/10.1109/MC.2021.3090018.
18. Bertino E. Zero Trust Architecture: Does It Help? // IEEE Security & Privacy. 19(05). P. 95-96, 2021. https://doi.org/10.1109/MSEC.2021.3091195.
19. Shackelford S. Zero-trust security: Assume that everyone and everything on the internet is out to get you – and maybe already has. The Conversation. URL: https://theconversation.com/zero-trust-security-assume-that-everyone-and-everything-on-the-internet-is-out-to-get-you-and-maybe-already-has-160969. (дата звернення: 10.07.2024).
20. The National Cyber Security Centre. Zero trust architecture design principles. Guidance. Version 1.0. 2021. URL: https://www.ncsc.gov.uk/collection/zero-trust-architecture. (дата звернення: 10.07.2024).
21. NIST Special publication 1800-35B. Implementing a Zero Trust Architecture. Vol. B: Approach, Architecture, and Security Characteristics. 2023. 264 p. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture. (дата звернення: 10.07.2024).
22. Rais R., Morillo C., Gilman E., Barth D. Zero Trust Networks. Building Secure Systems in Untrusted Networks. 2nd ed. O'Reilly Media, 2024. 332 p.
23. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey // IEEE Access. 2022. Vol. 10. P. 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679.
24. SDP Specification 1.0. Cloud Security Alliance (CSA). 2014. URL: https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0. (дата звернення: 10.07.2024).
25. Software-Defined Perimeter (SDP) Specification v2.0. Cloud Security Alliance (CSA). 2022. URL: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2. (дата звернення: 10.07.2024).
26. Nadeau T. D., Gray K. SDN: Software Defined Networks: An authoritative review of network programmability technologies. O'Reilly Media, Inc., 2013. 382 p.

27. Cohen R., Barabash K., Rochwerger B., Schour L., Crisan D., Birke R., ... & Jain V. An intent-based approach for network virtualization // Proc. 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013). IEEE. 2013. P. 42–50.

28. Bilger B., Boehme A., Flores B., Guterman Z., Hoover M., Iorga M., Islam J., Kolenko M., Koilpilla J., Lengyel G., Ludlow G., Schroeder T., Schweitzer J. Software defined perimeter working group. SDP specification 1.0. Cloud Security Alliance, Tech. Rep. 2014. URL: https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/. (дата звернення: 10.07.2024).

29. Koilpillai J., Garbis J., Islam J., Flores B., Bailey D., Chen B., Bremler E., Roza M., Mahmud S. Software-Defined Perimeter (SDP) Specification 2.0. Cloud Security Alliance, Tech. Rep. 2022. URL: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2. (дата звернення: 10.07.2024).

30. Ross R., Pillitteri V., Graubart, R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800–160. Vol. 2. Revision 1. 2021. 310 p.

31. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., ... & Zhou Y. Understanding the Mirai Botnet // 26th USENIX security symposium (USENIX Security 17). 2017. P. 1093–1110.

32. Mirai Botnet. URL: https://web.archive.org/web/20161212084605/https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet. (дата звернення: 10.07.2024).

33. Bursztein E. Inside the infamous Mirai IoT Botnet: A Retrospective Analysis. URL: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/. (дата звернення: 10.07.2024).

34. Anderson B., McGrew D. Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity // Proceedings of the 23rd ACM SIGKDD International Conference on knowledge discovery and data mining. 2017. P. 1723–1732. https://doi.org/10.1145/3097983.3098163.

35. American Council for Technology and Industry Advisory Council (ACT-IAC). Zero Trust Cybersecurity Current Trends. 2019. 29 p. URL: https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends. (дата звернення: 10.07.2024).

36. Cunningham C., Holmes D., Pollard J. The eight business and security benefits of zero trust. Forrester Research, Inc., 2019 URL: https://www.forrester.com/report/the-eight-business-and-security-benefits-of-zero-trust/RES134863. (дата звернення: 10.07.2024).

37. What is Cloud Native? URL: https://aws.amazon.com/what-is/cloud-native/?nc1=h_ls. (дата звернення: 10.07.2024).

38. Chandramouli R., Butcher Z. NIST Special Publication 800-207A. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. 2023. https://doi.org/10.6028/NIST.SP.800-207A.

39. NIST Special Publication 800-37 Revision 2. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy. https://doi.org/10.6028/NIST.SP.800-37r2.

40. Mullen-Schultz G. Blue/Green Deployment with Azure Front Door. URL: https://techcommunity.microsoft.com/t5/azure-architecture-blog/blue-green-deployment-with-azure-front-door/ba-p/1609178. (дата звернення: 10.07.2024).

41. He Y., Huang D., Chen L., Ni Y., Ma X. A survey on zero trust architecture: Challenges and future trends // Wireless Communications and Mobile Computing. 2022. 2022(1). 6476274. https://doi.org/10.1155/2022/6476274.

Надійшла до редколегії 15.09.2024

Відомості про авторів:

Єсін Віталій Іванович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

Вілігура Владислав Вікторович – Харківський національний університет імені В.Н. Каразіна, викладач кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

Узлов Дмитро Юрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, в.о. директора навчально-наукового інституту комп'ютерних наук та штучного інтелекту; Україна; e-mail: dmytro.uzlov@karazin.ua; ORCID: https://orcid.org/0000-0003-3308-424X