Zero Trust, або Керована параноя

Концепція змінилась: нині перспективніше не захищати мур, а перекопати вулиці.

Модель безпеки з нульовою довірою (Zero Trust) виходить з того, що систему вже зламано, і тому довіряти не можна нікому, навіть легітимним користувачам усередині периметра. А отже, кожен доступ до даних і програм потребує підтвердження. Окрім того, модель передбачає видачу користувачам лише мінімально необхідних привілеїв, а також профілювання їх поведінки для подальшого виявлення аномалій та загроз. Усе це має вберегти корпоративні ресурси навіть у випадку компрометації або хакерської атаки, адже, за задумом, зловмисник загрузне там, куди зміг проникнути, а вглиб корпоративної мережі його не пустять.

Zero Trust у багатьох на вустах після гучних витоків даних, а також з тієї причини, що з переходом співробітників на віддалений режим захист інформації помітно ускладнився. Цю модель впровадили у свої продукти всі ключові постачальники рішень безпеки. Зокрема, вона є складовою іншої популярної концепції — SASE. «СіБ» розбирався, як працює Zero Trust, що можуть запропонувати виробники і якими можуть бути сценарії застосування.

Від апріорної довіри до тотальної недовіри

Термін Zero Trust був запропонований ще у 2009 році аналітиком компанії ***Forrester*** Джоном Кіндервагом, який висловив тезу, що «довіра є вразливістю», і сформулював стратегію: «Ніколи не довіряй, завжди перевіряй». Це стало суттєвим відходом від традиційної моделі безпеки, де користувачі і пристрої всередині периметру за умовчанням вважаються благонадійними і отримують доступ скрізь. Тим самим будь-яка організація є вразливою до дій зловмисних інсайдерів і до атак хакерів, які, проникнувши за периметр, можуть швидко розійтись по всій мережі. Ця модель застаріла через широке використання хмарних сервісів, а також поширення віддаленого режиму роботи, особливо з початком пандемії (сам Forrester зараз просуває поняття Zero Trust eXtended — ZTX).

Gartner зауважує, що самим терміном Zero Trust нерідко зловживають у маркетингу безпекових продуктів, проте він все ж є корисним для позначення підходу, де принцип безумовної довіри вилучено з комп'ютерної інфраструктури. Натомість її рівень постійно обраховується і підлаштовується таким чином, щоб забезпечувати доступ до корпоративних ресурсів за принципом «рівно скільки і наскільки треба» («just-in-time, just-enough», так це звучить англійською). При цьому Gartner зазначає, що повної системи безпеки за принципом нульової довіри, можливо, ніколи не вдасться створити, а проте дещо можна починати впроваджувати вже зараз.

Сам Gartner використовує термін «Мережевий доступ з нульовою довірою» (Zero Trust Network Access — ZTNA), визначаючи його як «продукти і сервіси, що створюють базований на ідентифікаторах і контексті контур

логічного доступу, який охоплює собою користувача і програму або набір програм. Ці програми приховані від пошуку, а доступ можливий лише через довіреного брокера і для групи поіменованих сутностей».

Існує важливий документ Національного інституту стандартів і технологій США (***NIST***) за номером 800-207 і з лаконічною назвою Zero Trust Architecture, у якому розписано, що таке, власне, Zero Trust і як цей принцип втілювати в життя. Отже, NIST визначає концепцію нульової довіри як сукупність понять та ідей, призначених для мінімізації невизначеності та забезпечення прийняття точних рішень щодо доступу до інформаційних систем та послуг — строго за запитом і з найменшими привілеями — в умовах, коли мережа вважається скомпрометованою. А архітектура нульової довіри — це відповідно корпоративний план з кібербезпеки, який включає поняття нульової довіри і враховує взаємовідносини, планування робочих процесів і політики доступу. Мета всього цього — запобігти несанкціонованому доступу до сервісів та даних, а також забезпечити якомога більш деталізований контроль доступу.

Правила нульової довіри за NIST

NIST також прописує основоположні принципи Zero Trust. По-перше, ресурсами вважаються усі джерела даних і сервіси їх обробки. У тому числі до них належать SaaS-сервіси зберігання даних, промислові системи, що надсилають команди виконавчим механізмам, а також, залежно від політики безпеки, особисті пристрої співробітників, якщо вони мають доступ до корпоративних ресурсів.

Усі комунікації мають бути захищені незалежно від того, надходить запит з мережі чи ззовні, і при цьому доступ не повинен автоматично надаватися лише тому, що запит генерується зсередини периметру. Якщо ж доступ отримано, то з найменшими привілеями, необхідними для виконання завдання. А зі зміною завдання повинні відповідно змінюватися й привілеї. (Атаку Sunburst, яка вразила рік тому американські урядові установи і зачепила також інші країни, уможливили саме надмірні привілеї. Зрештою, те саме ми бачили у 2017 під час атаки NotPetya). Автентифікація та авторизація, здійснені для одного ресурсу, не повинні автоматично забезпечувати доступ до іншого.

Доступ до ресурсів визначається політикою, яка динамічно змінюється і може враховувати час і дату запиту, а також характеристики пристрою. Компанія ***CrowdStrike***, наприклад, наводить такий перелік цих характеристик: ідентифікатор і тип користувача (людина або програма); число привілеїв на пристрої; типові з'єднання (тобто поведінка); тип і призначення кінцевого пристрою; геолокація; версія прошивки; протокол автентифікації; версія ОС і останні оновлення; програми, встановлені на пристрої; зафіксовані інциденти, у тому числі підозріла активність та опізнані атаки.

Ще однією важливою вимогою в архітектурі нульової довіри є постійний моніторинг безпечності і благонадійності усіх власних і асоційованих пристроїв. Ті з них, які визнано скомпрометованими або які мають вразливості чи не керуються самою організацією (наприклад, BYOD), повинні мати інакші права, аніж ті, що належать компанії і вважаються безпечними. Взагалі повинен діяти безперервний цикл отримання прав доступу, сканування і оцінювання загроз, адаптації та постійної переоцінки довіри, постійного моніторингу з можливою реавтентифікацією та реавторизацією у разі, наприклад, запиту доступу до нових ресурсів або виявлення підозрілих дій. Одного дозволу на все життя просто недостатньо, тому що загрози і атрибути пристроїв користувачів постійно змінюються. При цьому компанія має збирати якомога більше інформації про стан пристроїв і мережевої інфраструктури, використовуючи її для покращення безпеки.

З точки зору планування корпоративної мережі наперед закладається принцип, що нападник вже знаходиться всередині. Якщо у корпоративних комунікаціях використовується інфраструктура, що не належить компанії (наприклад, публічна мережа

Wi-Fi для доступу віддалених співробітників), така мережа заздалегідь розглядається як ворожа, де увесь трафік може відстежуватись і потенційно модифікуватись.

Архітектура нульової довіри

У різних визначеннях, чи то від Gartner, NIST чи інших організацій, базова архітектура Zero Trust складається з двох компонентів. По-перше, це певний довірений шлюз чи проксі-сервер, який перехоплює запити на доступ до ресурсів і надалі за командою надає цей доступ або відмовляє. По-друге — контролер доступу, який здійснює автентифікацію і приймає рішення. Контролер зазвичай також поділяється на два компоненти, один з яких відповідає за аналіз даних, а інший видає команди шлюзові.

Логічна модель NIST, яка представлена на **рис. 1**, складається з компонентів, які можуть працювати локально або з хмари. Вона має три ключові складові. Механізм реалізації політик (Policy engine, PE) приймає остаточне рішення про надання доступу до ресурсу (або його відкликання), використовуючи дані з різних джерел і внутрішній алгоритм довіри. Він працює в парі з іншим компонентом — адміністратором політик (Policy Administrator, PA), що надає токен автентифікації та авторизації, за допомогою якого клієнт отримує доступ до ресурсів. Точка реалізації політик (Policy Enforcement Point, PEP) за командою від адміністратора створює і завершує з'єднання між клієнтом і ресурсом, а також здійснює його моніторинг. Цей компонент також може дробитись на клієнтську і серверну частини.

Рішення про надання доступу приймається на основі різних джерел, внутрішніх і зовнішніх. Тут відправною точкою є політики доступу до даних, які наперед прописані у PE або генеруються ним динамічно. Система безперервної діагностики і корекції (Continuous Diagnostics and Mitigation, CDM) збирає дані про стан усіх пристроїв у мережі і надає адміністратору інформацію, наприклад, про те, чи працює на пристрої операційна система з усіма останніми оновленнями, чи присутні на ньому не схвалені організацією програми і чи не має він якихось відомих уразливостей. CDM також відшукує сторонні пристрої, підключені до корпоративної мережі. Система інформації про ключову корпоративну інфраструктуру (Public Key Infrastructure, PKI) генерує та зберігає сертифікати, що видаються різним ресурсам, сервісам та програмам.

SIEM збирає інформацію про інциденти для подальшого аналізу, а кіберрозвідка (Threat Intelligence) — дані про віднайдені нові загрози та вразливості (наприклад, після повідомлення про атаку на певний ресурс можна взагалі заборонити доступ до нього). До інших джерел даних належать система відповідності галузевим стандартам (скажімо, про захист інформації), журнал усіх подій, зафіксованих у мережі, і система управління ідентифікацією, яка зберігає імена, адреси електронної пошти та інші атрибути користувачів.

NIST зауважує, що архітектура Zero Trust може різнитися залежно від потреб компанії, і прописує кілька таких основних варіацій. Одна з них полягає у ***посиленому управлінні обліковими даними*** (Enhanced Identity Governance). Тут головним критерієм доступу є привілеї, видані конкретному суб'єкту. Цей принцип підходить до компаній, які застосовують модель відкритої мережі з гостьовим доступом або великою кількістю власних пристроїв користувачів, що підключаються до мережі. У цьому разі доступ до самої мережі надається усім, але до корпоративних ресурсів — лише тим, хто має відповідні привілеї. Також ця модель добре працює у випадку, коли компанія використовує хмарні сервіси, де немає можливості розгорнути власні компоненти Zero Trust. Її недоліком є те, що зловмисники все ж можуть мандрувати мережею і займатися розвідкою або запускати DDoS-атаки.

Принцип ***мікросегментації*** передбачає розділення ресурсів на окремі групи, для чого використовуються інтелектуальні комутатори, NGFW або спеціальні шлюзи, що відіграють роль точок реалізації політик (хоча це можна влаштувати і за допомогою програмних агентів або мережевих екранів на кінцевих пристроях). Важливо, щоб шлюзи могли швидко змінювати конфігурацію, прилаштовуючись до нових загроз і варіацій потоків даних

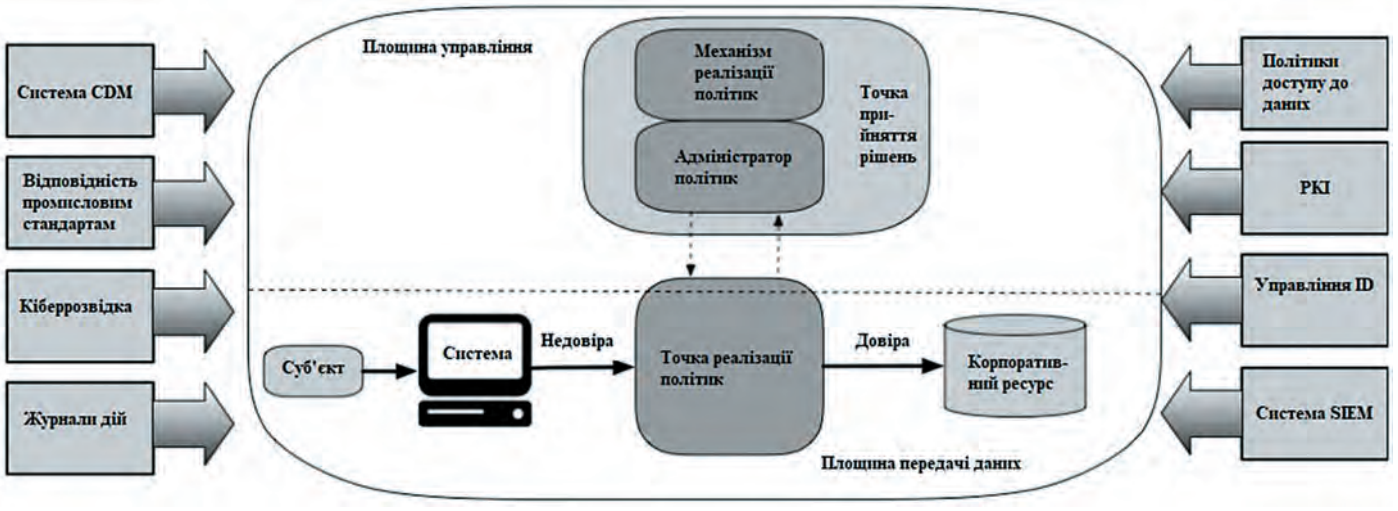

Рис. 1. Головні логічні компоненти моделі нульової довіри (джерело: NIST)

у мережі. Третій варіант полягає в організації ***програмно-визначуваних периметрів***, тут адміністратор виступає у ролі контролера, який динамічно змінює конфігурацію мережі на основі рішень, що їх приймає PE.

Рухаючись далі від абстрактної архітектури, NIST пропонує кілька більш конкретних варіантів її реалізації. Перший варіант — модель ***«Агент-шлюз»***, коли на кожному пристрої встановлюється програмний агент, який координує з'єднання, а кожен ресурс має такий самий програмний шлюз. Отримавши запит на доступ до ресурсу, агент скеровує його адміністратору, а той передає далі в механізм реалізації політик для оцінювання. У разі позитивної відповіді агент конфігурує з'єднання з відповідним шлюзом. У моделі ***«Анклав»*** шлюз розташовується не перед кожним ресурсом, а перед їх групою. Ця модель корисна для організацій, що мають власний дата-центр або застарілі ресурси (наприклад, бази даних без API-інтерфейсу).

У моделі ***«Портал»*** використовується самий лише шлюз, який слугує, власне, порталом до якогось ресурсу чи групи ресурсів (приватної хмари або ЦОД). Перевага цього варіанту полягає в тому, що не потрібно встановлювати програмний агент на кожен пристрій, а це зручно для BYOD і співпраці між компаніями. Хоча є й зворотна сторона медалі: система може збирати лише обмежену інформацію про пристрої, звідки надходять запити. Протилежний приклад являє собою модель ***«Пісочниця»***, де на користувацьких пристроях дозволені програми або процеси запускаються у ізольованому середовищі (на віртуальній машині абощо), щоб захистити їх від потенційно скомпрометованого пристрою. Тобто ці дозволені програми можуть надсилати запити на ресурси, але усі інші застосунки отримуватимуть відмову. Перевагою цього методу є те, що навіть коли пристрій не можна просканувати на наявність уразливостей, ізольовані програми будуть захищені від зловмисного ПО; з іншого боку, компанія повинна забезпечити роботу пісочниць на всіх пристроях, і при цьому вона також не матиме повної видимості цих пристроїв.

Сценарії

Ідея Zero Trust сягає корінням в територіально розподілені корпоративні мережі, що складаються з кількох об'єктів, не поєднаних фізичними каналами, які належать компанії. Наприклад, це може бути організація з центральним офісом і філіями, або яка має віддалених працівників, які користуються корпоративними або й власними пристроями. Це, як зазначає NIST, є найпоширенішим сценарієм для нульової довіри. Точка прийняття рішень зазвичай розташовується в хмарі, що забезпечує легкий до неї доступ звідусіль, а звернення до ресурсів здійснюється або через програмний агент, або через портал.

В іншому сценарії, який також набуває популярності, компанія, на додачу до власної локальної мережі, користується послугами кількох хмарних провайдерів: наприклад, програми можуть працювати в одній хмарі, а бази даних до них зберігатися в іншій. Для простоти управління і якісної роботи програм ресурси у різних хмарах мають комунікувати безпосередньо, а не через мережу компанії. За таких обставин межа між корпоративною і хмарною інфраструктурою втрачає сенс, і периметр стає програмно-визначуваним. Точки реалізації політик розташовуються безпосередньо у хмарі на вході до програм і джерел даних, і клієнт має до них доступ через вбудований агент або портал.

Ще один поширений сценарій передбачає, що на території компанії буває багато відвідувачів або ж вона користується послугами сторонніх підрядників (наприклад, відповідальних за опалення, вентиляцію і кондиціювання повітря). Цим людям потрібно надати доступ в Інтернет, але ізолювати від корпоративних ресурсів **(рис. 2).** У цьому разі також використовується програмно-визначуваний периметр, доступ здійснюється за допомогою агента або через портал, а сторонні особи можуть узагалі не бачити корпоративних сервісів, що унеможливлює розвідку.

Буває ситуація, коли дві організації працюють над спільним проєктом, і одна з них володіє базою даних, до якої треба забезпечити доступ партнерам, при цьому закривши від них решту ресурсів. Для цього потрібно забезпечити спільне управління, так щоб брокери обох сторін могли автентифікувати співробітників одна одної. Наприклад, для доступу до бази даних партнера потрібно буде встановити програмний агент цього партнера на пристрої користувачів.

Нарешті, п'ятий сценарій описує також поширену ситуацію, коли потрібно

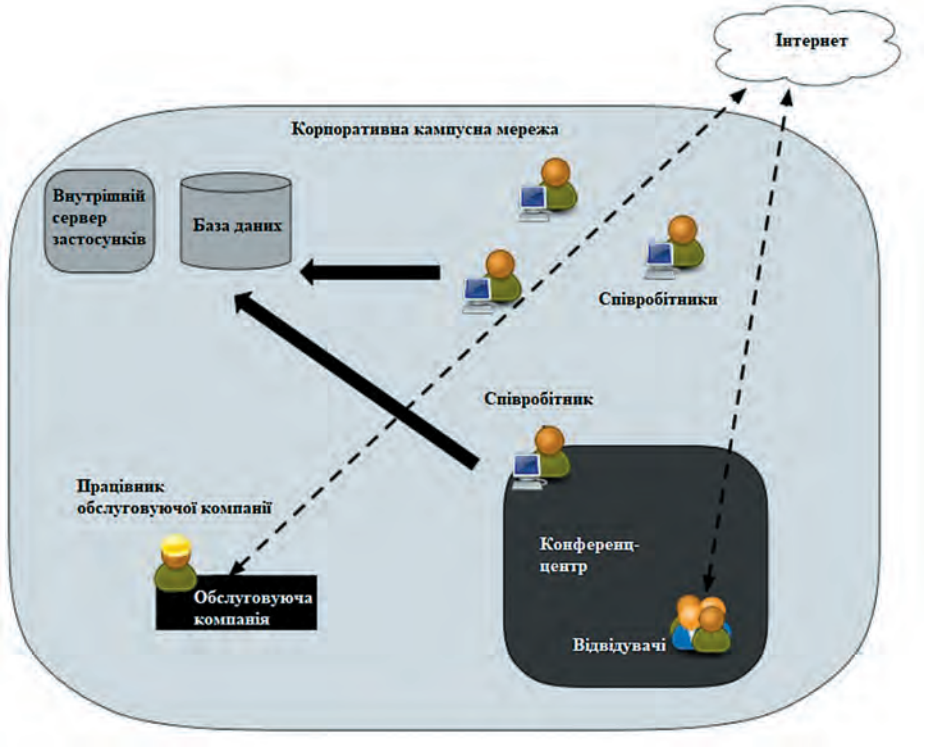

Рис. 2. Сценарій доступу з нульовою довірою за присутності сторонніх осіб (джерело: NIST)

встановити правила доступу для певної категорії користувачів (ділових партнерів або, наприклад, родичів співробітників). Тут знадобиться історія запитів, яка допоможе визначити приховану атаку: наприклад, різке збільшення спроб входу з невідомого браузера або з застарілої версії відомого, може свідчити про якусь автоматизовану спробу зламу.

Що вже є на ринку

Архітектура Zero Trust набула поширення відносно недавно, але її так чи інакше впровадили всі виробники безпекових рішень. Вона базується на існуючих продуктах, а іноді на нових придбаннях, зроблених спеціально з цією метою.

Forrester у своєму торішньому звіті Zero Trust eXtended Ecosystem Platform Providers наводить рейтинг таких виробників, зроблений, традиційно для цієї агенції, за трьома критеріями: поточна пропозиція, стратегія і присутність на ринку. Отже, до групи лідерів віднесені компанії Palo Alto Networks, MobileIron, Illumio, Appgate, Cisco і Akamai Technologies. Наступна категорія, «сильні гравці», включає 7 компаній, у тому числі Microsoft, Google і Forcepoint.

Отже, ***Palo Alto*** має повний набір продуктів для забезпечення нульової довіри будь-де: локально, в дата-центрі чи у хмарі. Для цього виробник останніми роками займався як створенням власних інструментів, так і їх купівлею. Архітектура Zero Trust побудована на таких рішеннях PAN, як, наприклад, платформа захисту для хмар Prisma Cloud і, зокрема, модуль Enterprise Infrastructure Entitlement Management (IAM), який контролює доступ до хмарних ресурсів, визначає ризиковані дозволи і забезпечує доступ з найменшими привілеями. Також сюди входять мережеві екрани наступного покоління і платформа розширеного виявлення та реагування на загрози кінцевим точкам Cortex XDR.

Cisco у 2018 році придбала компанію ***Duo Security***, що спеціалізувалася на мультифакторній автентифікації. Відтоді продукти Duo були інтегровані у портфель Cisco, внаслідок чого постала об'єднана архітектура для захисту «трьох W»: персоналу (Workforce) за допомогою Duo, робочого місця (Workplace) через SD-WAN і робочого трафіка (Workload), де рішення Tetration забезпечує сегментацію для програм у багатохмарних середовищах. Окрім того, Cisco пропонує послугу Zero Trust Strategy Service, в рамках якої оцінює особливості замовника і виробляє трирічний план переходу до моделі нульової довіри.

З тих виробників, які не увійшли до списку Forrester, але добре відомі українським користувачам, виділимо, наприклад, ***Fortinet***. В основі його архітектури лежить FortiAuthentificator, який виконує роль керівного центру і відповідає за автентифікацію (у тому числі багатофакторну), авторизацію і управління доступом. Рішення FortiToken використовується для двофакторної автентифікації і реалізується у вигляді апаратного токена або мобільного застосунку. Другою метою архітектури є безперервний моніторинг пристроїв у мережі і контролю доступу, для чого використовується рішення FortiNAC — воно виявляє усі пристрої, які підключені до мережі або намагаються підключитися, визначає, чи вони не скомпрометовані, і класифікує за роллю і призначенням. Нарешті, для безпечного віддаленого доступу слугує рішення FortiClient, яке створює VPN-тунелі.

У ***Check Point*** архітектура нульової довіри носить назву Infinity і також об'єднує існуючі рішення за кількома напрямками: захист мереж (шлюзи), робочого трафіка (CloudGuard), персоналу (Identity Awareness і CloudGuard SaaS), даних (рішення для шифрування та запобігання витокам) та пристроїв (зокрема, пісочниця SandBlast). Загалом Check Point Infinity використовує 64 різних засоби безпеки для захисту від відомих і невідомих загроз.

Недовіру цінують

В Інтернеті можна зустріти різні цифри, які свідчать про активне просування моделі Zero Trust. Наприклад, у звіті агенції ***Grand View Research*** від липня 2021 року йдеться, що до 2028 року світовий ринок Zero Trust сягне $59,43 млрд, а середнє річне зростання за цей період становитиме 15,2%. Markets&Markets вважає, що ринок зросте з $19,6 млрд у 2020 році до $51,6 млрд у 2026-му за темпів у 17,4% на рік.

Згідно з даними ***Statista*** на травень 2021 року, 72% респондентів запланували впровадження Zero Trust або вже й впровадили. Як ідеться у спільному звіті Gartner і китайської кібербезпекової компанії Qi-Anxin, до 2023 року 60% великих компаній відмовляться від VPN на користь ZTNA, а 40% використовуватимуть цю модель для інших цілей.

Торік компанія ***Pulse Secure*** провела дослідження серед 252 фахівців, що безпосередньо займаються мережевою сегментацією і безпечним віддаленим доступом. Серед опитаних 69% повідомили, що їхні організації мають намір упродовж року замінити існуючі технології віддаленого доступу на Zero Trust, у тому числі 27% вже це зробили. Лише 4% відповіли, що їхнє існуюче рішення повністю підтримуватиме Zero Trust, і ще 22% мали намір використовувати старі й нові технології разом. При цьому 43% повідомили, що під Zero Trust у них виділено кошти в рамках існуючих бюджетів, і 42% — з додатковим фінансуванням.

Оприлюднене навесні вже цього року дослідження ***Ponemon Institute***, проведене на замовлення ***Aruba***, показало, що серед трьох передових концепцій безпеки (SD-WAN, SASE і Zero Trust) саме остання відома найбільше (62% відповіли, що добре або дуже добре знайомі з нею). Темпи впровадження цієї концепції також є найвищими: 57% респондентів повідомили, що Zero Trust у них вже є або планується (**рис. 3**). При цьому серед тих 22% респондентів, які твердо переконані в ефективності своєї архітектури безпеки, темпи ще вищі: якщо загалом доля тих, хто вже впровадив Zero Trust або планує це зробити протягом року, становила 35%, то у передовій категорії — 48%.

Не довіряй і перевіряй

Zero Trust не є панацеєю і теж має свої вразливості. Зокрема, слабкою ланкою завжди залишається людина. Компоненти, які відповідають за прийняття рішень щодо доступу до ресурсів, потребують належного налаштування і обслуговування, тому багато залежить від персоналу, який може вносити зловмисні зміни або просто допускати помилки. Скомпрометований брокер,

Рис. 3. Плани впровадження Zero Trust серед організацій світу (дані Ponemon Institute)

відповідно, надаватиме доступ до ресурсів несхваленим пристроям. Тому будь-які зміни в конфігурації повинні заноситися в журнал.

За допомогою фішингу та інших засобів соціальної інженерії зловмисники можуть отримати доступ до цінних облікових записів (наприклад, бухгалтера або кадровика). Хакер, що заволодів легітимним записом (або й зловмисний інсайдер), може, своєю чергою, отримувати доступ до ресурсів, що є дозволеними для такого запису. З іншого боку, Zero Trust все ж не дозволить йому рухатися далі і відмовлятиме в доступі до ресурсів, де він не авторизований. Окрім того, контекстуальний алгоритм визначення довіри зрештою помітить незвичну поведінку і заблокує скомпрометований обліковий запис.

Іншу небезпеку можуть становити DDoS-атаки на компоненти архітектури нульової довіри. Цю загрозу можна зменшити, розташувавши відповідні компоненти у захищеній хмарі або розподіливши їх серед інфраструктури, але це, своєю чергою, створює нові ризики, адже відмова може статися на стороні вже хмарного провайдера (наприклад, теж через DDoS). Якщо адміністратор політик або шлюз доступу вийдуть з ладу, програми перестануть працювати. Альтернативно, якщо атака здійснюється власне на ресурси, а не на керівні компоненти Zero Trust, останні не зможуть сконфігурувати маршрут, оскільки самі ресурси будуть недоступні.

Зловмисники також можуть спробувати не лише заспамити, але й зламати брокера. Ймовірність цього невелика, якщо сервіс працює з хмари, де він захищений засобами провайдера, але у разі порушення ізоляції між хмарними орендаторами хакер зможе проникнути в системи клієнтів вендора, що надає сервіс ZTNA, зазначає Gartner. У цьому випадку потрібно негайно переключитися на резервного брокера, або, якщо це неможливо, просто відключитись від Інтернету.

Стримуючим фактором, як і багато де, є гроші. Markets&Markets зазначає, що вимоги до кібербезпеки зростають швидше, ніж заплановані бюджети. Більшості невеликих фірм бракує і грошей, і досвіду для запровадження передових концепцій кібербезпеки.

Gartner, втім, наводить низку варіантів, які можуть послужити альтернативою Zero Trust залежно від уподобань. Наприклад, сервіс Always-On VPN, який вимагає автентифікації користувачів і пристроїв. Віртуальний робочий стіл дозволяє «спроєктувати» корпоративну політику безпеки на віддалений пристрій, тоді як технологія ізоляції браузера забезпечує відокремлення Інтернет-сесій користувача від корпоративної мережі. У короткотерміновій перспективі експерти радять використовувати VPN і Zero Trust разом, де VPN слугує однією з технологій доступу.

Проте схоже, що у будь якому разі нічого кращого за повну недовіру для нинішніх умов поки не вигадали.

Василь ТКАЧЕНКО, СІБ

ХРОНИКА

Хакери атакували пристрої Apple у Гонконгу

Група аналізу загроз (Threat Analysis Group – TAG) виявила масову атаку типу «водопій» (watering hole) у Гонконгу. Щонайменше з серпня хакери, використовуючи вразливості у MacOS та iOS, встановлювали зловмисне ПО на пристрої користувачів, які відвідували сайти місцевої медійної організації та відомої продемократичної групи.

Яким чином хакери скомпрометували ці сайти, невідомо. Проте програма, яку вони встановлювали, працювала на пристроях жертв у фоновому режимі і могла скачувати файли або вивантажувати дані, робити знімки екрану і запис клавіатурного набору, вмикати аудіо запис і виконувати команди подібного типу. Окрім того, вона робила цифровий відбиток пристрою для подальшої ідентифікації.

Повідомляється, що атаки через iOS і MacOS різнилися за виконанням, проте обидві використовували вразливості нульового дня, про які Google повідомила Apple, а та їх негайно закрила. TAG не змогла проаналізувати повний ланцюжок атаки на пристрої iOS, проте визначила, що хакери експлуатували вразливість у браузері Safari. У випадку MacOS вони використали вразливість у браузерному рушієві WebKit (про яку раніше доповідала компанія Pangu Labs, проте дослідники Google віднесли її до zero-day, позаяк було невідомо, що вона працює і для цієї версії операційної системи), а також помилку системного ядра. Дослідники охарактеризували кампанію як «продукт ретельної соціальної інженерії».