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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення безпеки інформаційних систем організації на базі Zero Trust»

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

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

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

_____ Владислав КРАЄВСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
КРАЄВСЬКИЙ Владислав
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ZTNA – Zero Trust Network Access

ZTA – Zero Trust Architecture

ZTP – Zero Trust Platform

VPN – Virtual Private Network

FWaaS – Firewall as a Service

SIA – Secure Internet Access

SSA – Secure SaaS Access

IoT – Internet of Things

SIEM – Security Information and Event Management

IPS – Intrusion Prevention System

MFA – Multi-Factor Authentication

NAC – Network Access Control

NGFW – Next-Generation Firewall

PaaS – Platform as a Service

POPs – Points of Presence

SASE – Secure Access Service Edge

SWG – Secure Web Gateway

ВСТУП

Актуальність дослідження. В умовах швидкого розвитку цифрових технологій та постійного збільшення кількості кібератак на організації, проблема забезпечення інформаційної безпеки стає надзвичайно важливою. Технології захисту інформаційних систем повинні відповідати вимогам нових загроз, зокрема, у зв'язку з інтеграцією різноманітних платформ, віддаленими робочими процесами та використанням хмарних технологій. Одним із сучасних підходів до вирішення цієї проблеми є впровадження концепції Zero Trust, яка передбачає відсутність автоматичної довіри до користувачів, пристроїв і систем, незалежно від їхнього місцезнаходження або статусу в організаційній мережі.

Ідея нульової довіри (Zero Trust) стає важливою відповіддю на сучасні виклики в галузі кібербезпеки, оскільки традиційні методи захисту, що базуються на кордоні між внутрішньою та зовнішньою мережею, вже не здатні ефективно запобігти новітнім загрозам. Багато організацій сьогодні стикаються з необхідністю захисту не лише внутрішніх мереж, а й віддалених працівників, партнерів, а також інтеграції з хмарними сервісами та сторонніми ресурсами. У цьому контексті технологія Zero Trust дозволяє значно підвищити рівень захисту інформаційних систем шляхом постійної верифікації доступу та забезпечення контролю на кожному етапі взаємодії з корпоративними ресурсами.

Актуальність дослідження також зростає через постійне ускладнення атак, що спричиняють серйозні наслідки для діяльності організацій, включаючи витік конфіденційної інформації, фінансові збитки та репутаційні втрати. Враховуючи ці фактори, застосування Zero Trust у забезпеченні безпеки інформаційних систем є критично важливим для організацій будь-якого масштабу та напрямку діяльності.

Крім того, впровадження Zero Trust вимагає детального аналізу, правильного вибору інструментів і методів, що робить таке дослідження важливим для розвитку наукових знань у галузі інформаційної безпеки. Це дає змогу не лише покращити рівень захисту організаційних ресурсів, а й оптимізувати використання технологій

захисту в умовах сучасної цифрової економіки.

Об'єкт дослідження – забезпечення безпеки інформаційних систем організації.

Предмет дослідження – технологія забезпечення безпеки інформаційних систем організації на базі Zero Trust.

Мета роботи – розробити варіант застосування технології забезпечення безпеки інформаційних систем організації на базі Zero Trust.

Наукові завдання:

дослідити сутність проблеми забезпечення безпеки інформаційних систем організації на основі технології Zero Trust.

проаналізувати основні принципи та концепції Zero Trust у контексті безпеки інформаційних систем організацій.

оцінити існуючі підходи та методи забезпечення безпеки в рамках Zero Trust, застосовувані в сучасних організаціях.

дослідити основні технологічні інструменти для впровадження Zero Trust, зокрема методи багатофакторної автентифікації, управління доступом та перевірку пристроїв.

розробити рекомендації щодо впровадження технології Zero Trust для забезпечення безпеки інформаційних систем організації.

оцінити ефективність застосування Zero Trust для забезпечення безпеки організацій в умовах віддаленої роботи, хмарних технологій та мобільного доступу.

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

Практичне значення одержаних результатів: запропоновано варіант застосування технології забезпечення безпеки інформаційних систем на базі Zero Trust, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

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

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЇ

1.1. Дослідження основних загроз інформаційних систем організації

У сучасному світі, який стає все більш цифровим, кібербезпека стала критичною проблемою для окремих осіб, організацій та урядів. Зі стрімким розвитком технологій також спостерігалося експоненціальне зростання кіберзагроз і атак. Тому важливо постійно відстежувати та аналізувати нові загрози в кібербезпеці, щоб бути на крок попереду цих зловмисників. Кібербезпека стосується практики захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж і даних від цифрових атак і несанкціонованого доступу. Він охоплює широкий спектр заходів і технологій, спрямованих на захист окремих осіб, організацій і навіть держав від кіберзагроз. Останніми роками сфера кібербезпеки стає дедалі складнішою та складнішою через швидкий розвиток технологій і стратегії кіберзлочинців, що постійно розвиваються. З кожним днем виявляються нові загрози та вразливості, що становить значний ризик для пристроїв, мереж і конфіденційної інформації.

Розуміння нових загроз у кібербезпеці має вирішальне значення для розробки ефективних стратегій протидії та пом'якшення ризиків. Виявляючи останні вектори атак, організації можуть проактивно впроваджувати надійні заходи безпеки та навчати своїх співробітників найкращим практикам захисту конфіденційної інформації. Люди також можуть вжити заходів для підвищення своєї особистої кібербезпеки, наприклад використовувати надійні паролі, регулярно оновлювати програмне забезпечення та бути обережними щодо підозрілих електронних листів або веб-сайтів. Щоб усунути ці нові загрози, фахівці з кібербезпеки повинні постійно бути в курсі останніх новин. тенденції, вразливості та методи атак. Їм потрібно прийняти багаторівневий підхід до захисту, який поєднує в собі технологічні рішення, навчання співробітників і проактивну розвідку про загрози. Крім того, співпраця між урядами, підприємствами та окремими особами має вирішальне значення для розробки ефективних стратегій кібербезпеки та обміну інформацією про нові загрози.

Загрози кібербезпеці можуть мати значний вплив на фінансові втрати для окремих осіб і організацій. Є кілька способів, якими ці загрози можуть призвести до фінансових втрат. По-перше, кібератаки можуть призвести до прямого фінансового крадіжки. Хакери можуть отримати несанкціонований доступ до фінансових систем і викрасти гроші чи конфіденційну фінансову інформацію. Це може призвести до значних фінансових втрат для окремих осіб і підприємств, оскільки їм, можливо, доведеться відшкодовувати вкрадені кошти або зіткнутися з правовими наслідками, пов'язаними з фінансовим шахрайством. Більше того, загрози кібербезпеці також можуть спричинити фінансові втрати через збої в бізнесі. Атаки програм-вимагачів, наприклад, можуть шифрувати файли та системи, роблячи їх недоступними, доки не буде сплачено викуп. Це може призвести до значних простоїв, втрати продуктивності та потенційної втрати прибутку для підприємств. Крім того, організаціям може знадобитися інвестувати в заходи з усунення несправностей і відновлення, що може додатково збільшити фінансовий тиск. Іншим впливом загроз кібербезпеці на фінансові втрати є вартість регулятивних штрафів і судових зборів. Порушення даних та інші кіберінциденти часто призводять до розслідувань регуляторними органами. Недотримання правил захисту даних може призвести до великих штрафів, що може суттєво вплинути на фінансовий стан організації. Крім того, організації також можуть нести витрати на наймання юридичного радника для ознайомлення з правовими наслідками та потенційними судовими позовами, пов'язаними з порушенням кібербезпеки. Нарешті, існують також непрямі фінансові втрати, які можуть виникнути в результаті загроз кібербезпеці. До них відноситься репутаційна шкода та втрата довіри клієнтів. Якщо заходи організації з кібербезпеки не є адекватними, і вона страждає від витоку даних або іншого кіберінциденту, це може призвести до негативного розголосу та заплямованої репутації. Це може призвести до втрати довіри та лояльності клієнтів, що призведе до зниження продажів або відтоку клієнтів. Відновлення довіри та відновлення зіпсованої репутації може бути дорогим і тривалим процесом.

Шкода репутації

Загрози кібербезпеці можуть мати значний вплив на репутацію компанії. Коли компанія зазнає витоку даних або стає об'єктом кібератаки, це може зашкодити довірі

клієнтів і зацікавлених сторін до організації. Однією з головних проблем клієнтів є захист їх особистої інформації. Якщо компанія не в змозі належним чином захистити дані клієнтів і вони скомпрометовані, це може створити відчуття незахищеності серед клієнтів. Це може призвести до втрати бізнесу, оскільки клієнти можуть вирішити перевести свій бізнес в інше місце, побоюючись, що їхня інформація може бути небезпечною для постраждалої компанії. Крім того, клієнти можуть вважати компанію недбалою або некомпетентною з точки зору кібербезпеки, що ще більше шкодить її репутації. Окрім впливу на клієнтів, загрози кібербезпеці також можуть мати наслідки для відносин компанії з її зацікавленими сторонами. Постачальники, партнери та інвестори можуть поставити під сумнів здатність компанії захистити конфіденційну інформацію та вагатися щодо продовження ведення бізнесу з компанією. Це може призвести до втрати цінних партнерських відносин і фінансової підтримки, що ще більше завдасть шкоди репутації компанії. Крім того, на суспільне сприйняття компанії після інциденту кібербезпеки також може вплинути висвітлення в ЗМІ та громадський контроль. Те, як компанія реагує на злом або кібератаку, може сильно вплинути на її репутацію. Якщо компанія повільно реагує, не забезпечує прозору та своєчасну комунікацію або применшує серйозність інциденту, це можна розглядати як спробу приховати правду або не сприйняття ситуації серйозно. Це може призвести до негативної преси, негативної реакції громадськості та втрати довіри з боку громадськості. Зрештою, шкода репутації компанії через загрози кібербезпеці може мати довгострокові наслідки. Щоб відновити довіру та позитивний імідж в очах клієнтів і зацікавлених сторін, можуть знадобитися роки. Це може призвести до фінансових втрат, труднощів із залученням нових клієнтів і погіршення ділових відносин. Тому для компаній вкрай важливо інвестувати в заходи кібербезпеки та мають комплексний план реагування на інциденти, щоб мінімізувати вплив кіберзагроз на їхню репутацію.

Порушення конфіденційності

Вплив загроз кібербезпеці та вторгнення в конфіденційність є далекосяжним і може мати серйозні наслідки для окремих осіб, підприємств і суспільства в цілому .Перш за все, загрози кібербезпеці можуть призвести до несанкціонованого доступу до особистих і конфіденційних інформації. Це може призвести до крадіжки особистих

даних, фінансового шахрайства та інших форм кіберзлочинності. Люди можуть втратити доступ до своїх банківських рахунків, дані кредитної картки можуть бути викрадені або їхня репутація в Інтернеті буде пошкоджена. Це може мати довгострокові фінансові та емоційні наслідки для окремих людей та їхніх сімей. Крім того, компанії та організації також знаходяться під загрозою кібербезпеки. Порушення даних може призвести до втрати інформації про клієнтів, комерційної таємниці та інтелектуальної власності. Це може завдати шкоди репутації компанії, призвести до фінансових втрат і навіть призвести до судових позовів. Зокрема, малі підприємства часто стають мішенями кіберзлочинців, оскільки вони можуть мати менш складні заходи безпеки. Окрім фінансового впливу, вторгнення в конфіденційність через загрози кібербезпеці може підірвати довіру та підірвати особисті свободи. Люди можуть побоюватися участі в онлайн-діяльності, такій як електронна комерція чи соціальні мережі, через побоювання, що їхню конфіденційну інформацію буде скомпрометовано. Це може перешкоджати зростанню цифрової економіки та обмежувати потенціал для інновацій та підключення.

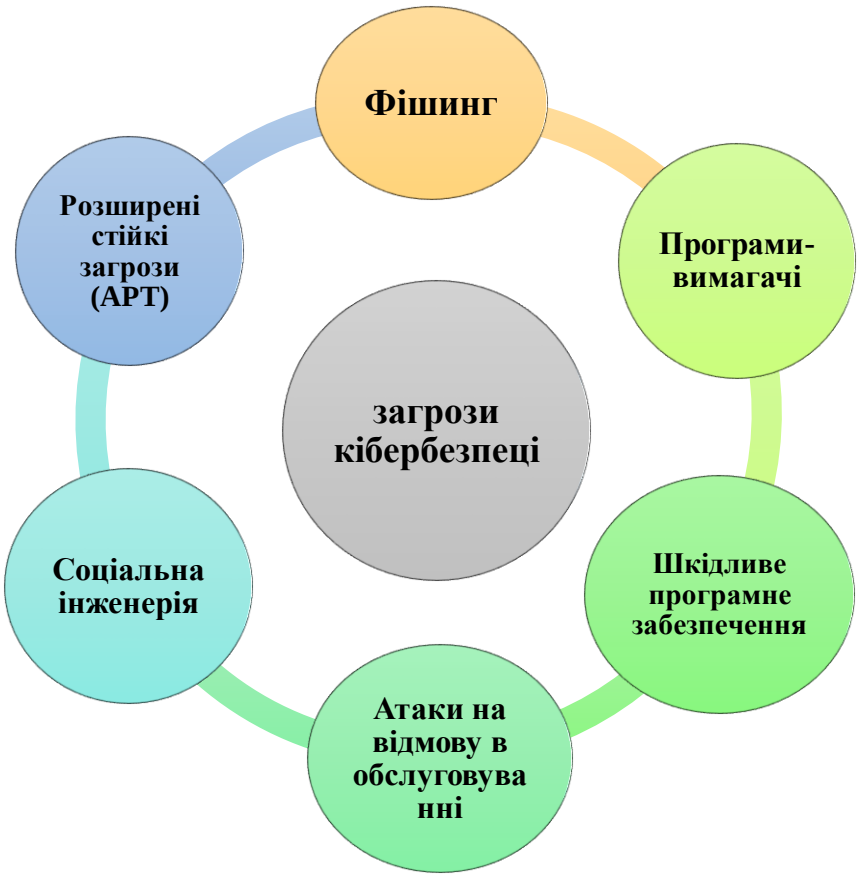

Рис.1.1. Основні загрози кібербезпеки

Типи загроз кібербезпеці

1. Шкідливе програмне забезпечення

Зловмисне програмне забезпечення означає шкідливе програмне забезпечення, яке є будь-яким програмним забезпеченням, призначеним для шкоди або використання комп'ютерів або комп'ютерних мереж. Зловмисне програмне забезпечення може включати віруси, хробаки, трояни, програми-вимагачі, шпигунські програми, рекламні програми та інші шкідливі програми. Зазвичай він поширюється через вкладення електронної пошти, завантаження програмного забезпечення, заражені веб-сайти або вразливе програмне забезпечення. Після встановлення на комп'ютер зловмисне програмне забезпечення може викрадати конфіденційну інформацію, пошкоджувати або видаляти файли, порушувати роботу системи та надавати несанкціонований доступ до мережі. Для захисту від цих загроз важливо встановити на комп'ютері хороше антивірусне програмне забезпечення та програмне забезпечення для захисту від зловмисного програмного забезпечення.

2. Соціальна інженерія

Соціальна інженерія – це метод, який використовують зловмисники, щоб змусити людей розкрити конфіденційну інформацію або виконати дії, які можуть поставити під загрозу безпеку. Це передбачає маніпулювання поведінкою людей і завоювання їх довіри, щоб обманом змусити їх розкрити особисту інформацію, як-от паролі чи фінансову інформацію, або змусити їх виконувати дії, які вони зазвичай не робили б, наприклад відкривати шкідливі вкладення електронної пошти або натискати посилання.

Атаки соціальної інженерії можуть мати різні форми, такі як фішингові електронні листи чи телефонні дзвінки, які видають себе за законних організацій чи осіб, видаючи себе за колег чи IT-персоналу або створюючи підроблені веб-сайти чи профілі в соціальних мережах, щоб завоювати довіру. Зловмисники також можуть особисто використовувати методи соціальної інженерії, наприклад «переслідування» (слідування за кимось у безпечну зону без належного дозволу) або перетекстування (створення хибного сценарію, щоб завоювати довіру та маніпулювати кимось, щоб поділитися інформацією). Цілі атак соціальної інженерії можуть бути різними. але часто включають крадіжку особистих даних, фінансове шахрайство,

несанкціонований доступ до систем або мереж або розповсюдження зловмисного програмного забезпечення чи програм-вимагачів. Захист від соціальної інженерії атаки передбачає обізнаність, скептицизм і освіту. Важливо завжди бути обережним, надаючи особисту інформацію або виконуючи дії, які загрожують безпеці. Обізнаність із загальними методами соціальної інженерії та попередженнями може допомогти людям ідентифікувати ці атаки та уникнути їх жертв. Організації також можуть впроваджувати такі заходи безпеки, як навчання співробітників тому, як розпізнавати атаки соціальної інженерії та реагувати на них, запроваджувати багатофакторну автентифікацію та регулярно оновлювати протоколи та системи безпеки.

3. Фішинг

Фішинг — це метод кіберзлочинності, коли зловмисники видають себе за юридична особа чи організація, як-от банк або постачальник онлайн-послуг, щоб обманом змусити осіб надати конфіденційну інформацію, таку як паролі або номери кредитних карток. Поширені методи фішингу включають надсилання шахрайських електронних листів або створення підроблених веб-сайтів, які дуже схожі на законні. Щойно зловмисник отримає викрадену інформацію, він може використати її для різних зловмисних цілей, наприклад для викрадення особистих даних або фінансового шахрайства. Фішингові атаки є значною загрозою для окремих осіб і організацій, тому важливо пам’ятати про ознаки фішингу, такі як підозрілі запити електронної пошти або незнайомі URL-адреси веб-сайтів, щоб захистити себе від того, щоб стати жертвою цих шахраїв.

4. Програми-вимагачі

Програми-вимагачі — це тип шкідливого програмного забезпечення (зловмисного ПЗ), яке шифрує файли жертви, роблячи їх недоступними та потім вимагає викуп в обмін на ключ дешифрування. Він призначений для вимагання грошей від окремих осіб, організацій або навіть урядів. Атаки програм-вимагачів зазвичай відбуваються через фішингові електронні листи, зловмисні завантаження або використання вразливостей у програмному забезпеченні чи системах. Після того, як файли жертви зашифровано, програма-вимагач відобразить повідомлення з інструкціями жертви про те, як сплатити викуп, зазвичай у формі криптовалюти, такої

як біткойн. Зловмисники можуть погрожувати видалити ключ дешифрування або назавжди знищити файли, якщо викуп не буде сплачено протягом заданого періоду часу. Атаки програм-вимагачів можуть мати серйозні наслідки, спричиняючи фінансові втрати, витік даних і навіть порушення критичної інфраструктури. Дуже важливо регулярно створювати резервні копії файлів і систем, оновлювати програмне забезпечення та бути обережним щодо підозрілих електронних листів або завантажень, щоб захиститися від атак програм-вимагачів.

5. Атаки на відмову в обслуговуванні

DoS атака – це тип кібератаки, під час якої зловмисник навмисно заповнює мережу, сервер або веб-сайт надмірним трафіком або даними для переповнює його ресурси та робить його недоступним для користувачів. Мета DoS-атаки полягає в тому, щоб порушити нормальне функціонування цільової системи чи мережі, зробивши її недоступною або спричинивши її збій. DoS-атаки можна здійснити різними способами, включаючи затоплення цілі високою кількість мережевих запитів, використання вразливостей у цільовому програмному забезпеченні чи інфраструктурі або використання ботнетів (мереж скомпрометованих комп’ютерів) для перевантажувати ціль трафіком із кількох джерел. Для організацій надзвичайно важливо мати комплексний план реагування на інциденти, щоб швидко пом’якшити наслідки DoS-атаки та мінімізувати шкоду. Це може включати процедури ізоляції уражених систем, сповіщення відповідних зацікавлених сторін і співпрацю з правоохоронними органами, якщо це необхідно.

6. Розширені стійкі загрози (APT)

Розширені стійкі загрози (APT) стосуються цілеспрямованих кібератак, які здійснюються добре фінансованими та добре фінансованими. кваліфіковані хакери, часто актори національної держави, з наміром отримати несанкціонований доступ до конкретного мережа або система організації. APT характеризуються своєю наполегливістю, оскільки зловмисники можуть продовжувати свої операції протягом тривалого періоду часу для досягнення своїх цілей. APT зазвичай включають кілька етапів, включаючи початкову розвідку та проникнення, встановлення плацдармів, пересування по мережі та викрадання або маніпулювання конфіденційними даними. Зловмисники використовують складні методи, щоб уникнути виявлення, наприклад

використання спеціального шкідливого програмного забезпечення, уразливостей нульового дня та тактик соціальної інженерії. APT зазвичай включають кілька етапів, включаючи початкову розвідку та проникнення, встановлення плацдармів, пересування по мережі та вилучення або маніпулювання конфіденційними даними. Зловмисники використовують складні методи, щоб уникнути виявлення, наприклад використання спеціального шкідливого програмного забезпечення, уразливостей нульового дня та тактик соціальної інженерії.

Мотиви, що стоять за APT, різні, але зазвичай включають збір розвідданих, викрадення інтелектуальної власності, шпигунство або порушення критичної інфраструктури. Цільові організації, як правило, володіють цінною та конфіденційною інформацією, як-от державні установи, оборонні підрядники, фінансові установи та компанії, що займаються дослідженнями та розробками (Raina, 2018). Для захисту від APT організації повинні впроваджувати комплексні заходи безпеки, включаючи сегментацію мережі, надійний контроль доступу, регулярні оцінки вразливості та навчання співробітників найкращим практикам безпеки. Крім того, аналіз загроз і розширені технології виявлення можуть допомогти вчасно ідентифікувати APT і реагувати на них [1].

1.2. Аналіз підходів до забезпечення безпеки інформаційних систем

Загрози кібербезпеці впливають на бізнес, уряд, некомерційні групи та людей. Дослідники та експерти з інформаційної безпеки регулярно працюють над створенням проактивних методів і інструментів для покращення кібербезпеки.

Атаки програм-вимагачів і слабкі місця внаслідок збільшення використання хмарних служб є деякими новими загрозами. Потенційна вразливість технології 5G і еволюція Інтернету речей (IoT), яка включає в себе розумні домашні пристрої, також становлять ризики для безпеки.

Загрози кібербезпеці стимулюють розвиток новітніх технологій у цій галузі. Далі розглядаються перспективні технології, які були розроблені для протидії актуальним кіберзагрозам.

Наведено опис найпоширеніших інноваційних рішень у сфері кібербезпеки, із зазначенням принципів їхньої роботи та основних напрямів застосування. Зазначені інструменти використовуються для захисту інформаційних систем від загроз, що постійно еволюціонують, і забезпечення надійного функціонування інформаційної інфраструктури.

Behavioral Analytics

Поведінкова аналітика аналізує дані, щоб зрозуміти, як люди поводяться на веб-сайтах, у мобільних додатках, системах і мережах. Фахівці з кібербезпеки можуть використовувати платформи поведінкової аналітики для пошуку потенційних загроз і вразливостей.

Аналіз моделей поведінки може призвести до виявлення незвичних подій і дій, які можуть вказувати на загрози кібербезпеці.

Наприклад, поведінкова аналітика може виявити, що з одного пристрою надходить надзвичайно велика кількість даних. Це може означати, що кібератака насувається або активно відбувається. Інші показники зловмисної діяльності включають незвичайний час подій і дій, які відбуваються в незвичній послідовності.

Переваги використання поведінкової аналітики включають раннє виявлення потенційних атак і можливість передбачити майбутні атаки. Організації можуть автоматизувати виявлення та реагування за допомогою поведінкової аналітики.

Блокчейн

Блокчейн — це тип бази даних, яка безпечно зберігає дані в блоках. Він з’єднує блоки за допомогою криптографії. Блокчейн дозволяє збирати інформацію, але не редагувати чи видаляти.

Фахівці з кібербезпеки можуть використовувати блокчейн для захисту систем або пристроїв, створювати стандартні протоколи безпеки та практично унеможливлювати проникнення хакерів у бази даних.

Переваги блокчейну включають кращу конфіденційність користувачів, зменшення людської помилки, більшу прозорість та економію коштів за рахунок усунення необхідності перевірки третьою стороною.

Блокчейн також усуває проблему безпеки зберігання даних в одному місці. Натомість дані зберігаються в мережах, що призводить до децентралізованої системи, яка менш вразлива для хакерів.

Проблеми використання блокчейну включають вартість і неефективність технології.

Cloud Encryption

Хмарні послуги підвищують ефективність, допомагають організаціям пропонувати покращені віддалені послуги та економлять гроші. Однак віддалене зберігання даних у хмарі може збільшити вразливість даних. Технологія хмарного шифрування перетворює дані зі зрозумілої інформації на нечитабельний код, перш ніж вони надходять у хмару.

Фахівці з кібербезпеки використовують математичний алгоритм для завершення хмарного шифрування. Лише авторизовані користувачі з ключем шифрування можуть розблокувати код, роблячи дані знову читабельними. Цей обмежений доступ мінімізує ймовірність витоку даних неавторизованими зловмисниками.

Експерти погоджуються, що хмарне шифрування є чудовою технологією кібербезпеки для захисту даних. Хмарне шифрування може запобігти неавторизованим користувачам отримати доступ до придатних для використання даних. Хмарне шифрування також може підвищити довіру клієнтів до хмарних служб і полегшити компаніям дотримання державних постанов.

Контекстно-залежна безпека

Контекстно-залежна безпека – це тип технології кібербезпеки, яка допомагає компаніям приймати кращі рішення щодо безпеки в режимі реального часу.

Традиційні технології кібербезпеки оцінюють, чи дозволити комусь доступ до системи чи даних, ставлячи питання «так/ні». Цей простий процес може призвести до того, що деяким законним користувачам буде відмовлено, що сповільнить продуктивність.

Контекстно-залежний захист зменшує ймовірність заборони входу авторизованому користувачеві. Замість того, щоб покладатися на відповіді на статичні запитання «так/ні», контекстно-залежна безпека використовує різну

допоміжну інформацію, як-от час, місцезнаходження та репутацію URL-адреси, щоб оцінити, чи є користувач законним чи ні.

Контекстно-залежна безпека оптимізує процеси доступу до даних і спрощує роботу законних користувачів. Однак питання конфіденційності кінцевих користувачів є проблемою.

Штучний інтелект (AI)

Фахівці з кібербезпеки можуть використовувати оборонний штучний інтелект (ШІ), щоб виявляти або зупиняти кібератаки. Кмітливі кіберзлочинці використовують такі технології, як образливий штучний інтелект і змагальне машинне навчання, оскільки традиційним інструментам кібербезпеки їх складніше виявити.

Образливий ШІ включає глибокі фейки, фальшиві зображення, персонажі та відео, які переконливо зображують людей або речі, яких ніколи не було або не існує. Зловмисники можуть використовувати змагальне машинне навчання, щоб обманом змусити машини вийти з ладу, надаючи їм неправильні дані.

Професіонали з кібербезпеки можуть використовувати захисний штучний інтелект, щоб виявляти та зупиняти атакуючий штучний інтелект, щоб він міг вимірювати, тестувати та вивчати, як функціонує система чи мережа.

Захисний штучний інтелект може посилити алгоритми, ускладнюючи їх зламати. Дослідники кібербезпеки можуть проводити жорсткіші тести на вразливість моделей машинного навчання.

Розширене виявлення та реагування (Extended detection and response - XDR)

Розширене виявлення та реагування (XDR) — це тип передової технології кібербезпеки, яка виявляє загрози безпеці та інциденти та реагує на них. XDR реагує на кінцеві точки, хмару та мережі. Він розвинувся з більш простого традиційного виявлення кінцевої точки та відповіді.

XDR надає більш цілісну картину, створюючи зв’язки між даними в різних місцях. Ця технологія дозволяє фахівцям з кібербезпеки виявляти й аналізувати загрози на вищому автоматизованому рівні. Це може допомогти запобігти або мінімізувати поточні та майбутні витоки даних у всій екосистемі активів організації.

Фахівці з кібербезпеки можуть використовувати XDR, щоб реагувати на цілеспрямовані атаки та виявляти їх, автоматично підтверджувати та співставляти

попередження та створювати комплексну аналітику. Переваги XDR включають автоматизацію повторюваних завдань, ефективне автоматизоване виявлення та зменшення кількості інцидентів, які потребують розслідування.

Manufacturer Usage Description (MUD)

Опис використання від виробника (MUD) — це стандарт, створений Інженерною робочою групою Інтернету для посилення безпеки пристроїв Інтернету речей у малих підприємствах і домашніх мережах.

Пристрої IoT вразливі до мережевих атак. Ці атаки можуть призвести до втрати особистих даних або призвести до припинення належної роботи машини. Пристрої IoT мають бути безпечними, не коштуючи надто дорого чи надто складно.

Переваги використання MUD включають просте, доступне покращення безпеки для пристроїв IoT. Фахівці з кібербезпеки можуть використовувати MUD, щоб зробити пристрої більш захищеними від розподілених атак на відмову в обслуговуванні. MUD може допомогти зменшити кількість пошкоджень і втрати даних у разі успішної атаки.

Zero Trust

Традиційна мережева безпека дотримувалася девізу «довіряй, але перевіряй», припускаючи, що користувачі в межах периметра мережі організації не є зловмисними загрозами. Нульова довіра, з іншого боку, узгоджується з девізом «ніколи не довіряй, завжди перевіряй».

Платформа для забезпечення безпеки мережі Zero Trust змушує всіх користувачів пройти автентифікацію, перш ніж отримати доступ до даних або програм організації.

Нульова довіра не передбачає, що користувачі всередині мережі заслуговують більше довіри, ніж будь-хто інший. Такий ретельніший контроль за всіма користувачами може призвести до підвищення загальної безпеки інформації для організації.

Фахівці з кібербезпеки можуть використовувати Zero Trust, щоб більш безпечно справлятися з віддаленими працівниками та проблемами, такими як загрози програм-вимагачів. Структура Zero Trust може поєднувати різні інструменти, включаючи багатофакторну автентифікацію, шифрування даних і безпеку кінцевої точки.

Регулювання

Оскільки частота кібератак продовжує значно зростати з кожним роком, уряди починають використовувати та пропагувати найкращі нормативні документи. У минулому уряди не часто втручалися в питання кібербезпеки.

Журнал Security Magazine, галузеве видання для професіоналів з кібербезпеки, прогнозує, що 2022 рік стане роком, коли уряди почнуть відігравати більшу роль у регулюванні того, як організації забезпечують безпеку інформації користувачів.

Потенційні регуляторні зміни включають виконавчі накази щодо стандартів кібербезпеки для державних постачальників, штрафи для компаній, які не дотримуються найкращих практик, збільшення попиту на кіберстрахування та закони про розкриття програм-вимагачів. Посилене регулювання, швидше за все, призведе до покращення стандартів безпеки [2].

1.3. Аналіз моделей доступу

У будь-якій організації необмежений доступ до систем і ресурсів створює значні ризики для безпеки. Нещодавні події в галузі кібербезпеки показали, що зловмисники будуть націлені на будь-яку організацію будь-якого розміру. Найпоширенішим вектором атаки є неавторизований доступ до законного облікового запису, якому часто передує фішинг атаки.

Для захисту від несанкціонованого доступу важливо встановити правила та політики для автентифікації та авторизації користувачів. Контроль доступу служить механізмом для встановлення цих засобів захисту, визначаючи, кому або чому дозволено виконувати дії або отримувати доступ до ресурсів в організації.

Керуючись вимогами безпеки, інфраструктурними міркуваннями та вимогами відповідності, компанії впроваджують заходи контролю доступу для своїх співробітників. Однак контроль доступу виходить за межі користувачів, охоплюючи також системні процеси та програми.

Новіші форми контролю доступу покращили безпеку шляхом заміни традиційних систем передовими методами, такими як ключ-карти та біометрія. Ці системи пропонують зручність авторизованим користувачам і забезпечують гнучкі

віддалені операції за допомогою хмарних рішень. Вони спрощують керування безпекою, автоматично оновлюючи бази даних користувачів і забезпечуючи детальний контроль доступу на основі ролей. Інтеграція з іншими системами безпеки покращує загальний захист, забезпечуючи комплексне спостереження та можливості визначення ситуації.

Типи моделей контролю доступу

Різноманітні моделі контролю доступу регулюють доступ до ресурсів в організаціях, визначаючи правила та механізми надання, відмови або скасування прав доступу. Ці моделі працюють на певних принципах, забезпечуючи різні рівні деталізації та гнучкості в управлінні дозволами.

Обов'язковий контроль доступу (MAC)

Обов’язковий контроль доступу (MAC) використовує централізований підхід до управління, що вказує на найвищий ступінь доступного контролю. Ця модель надає одноосібні повноваження щодо керування доступом власнику та зберігачу, позбавляючи кінцевих користувачів можливості надавати привілеї комусь іншому. Він призначає мітки безпеки ресурсам і користувачам, враховуючи класифікацію, дозвіл і розділення, тим самим обмежуючи доступ, якщо мітки не співпадають. Спочатку розроблений для військових і розвідувальних служб, MAC захищає конфіденційні дані в різних секторах, включаючи фінанси та уряд.

MAC використовує дві ключові моделі безпеки: Biba та Bell-LaPadula.

- Biba підкреслює цілісність інформації, дозволяючи суб’єктам очищення нижчого рівня читати інформацію вищого рівня («читати»), а суб’єктам вищого рівня писати для об’єктів очищення нижчого рівня («записувати»). Ця модель підходить для бізнес-контексту, полегшуючи спілкування між керівниками та працівниками нижчого рівня.
- Bell-LaPadula надає пріоритет конфіденційності та зазвичай застосовується в урядових або військових ролях. Користувачі з вищим рівнем допуску, наприклад, Цілком таємно, мають право писати на своєму або вищому рівні («записати»), тоді як їм дозволено читати інформацію на нижчих рівнях («читати вниз»). Ця модель забезпечує строгий контроль над доступом на основі рівнів дозволу.

Переваги

- Суворе дотримання правил, оскільки користувачі не можуть перевизначати загальноорганізаційні політики, встановлені адміністраторами MAC.
- Ефективна категоризація ресурсів за допомогою міток безпеки, обмеження доступу до певних груп користувачів.

Недоліки

- Перешкоджає співпраці через суворі заходи безпеки.
- Комплексне виконання.
- Збільшене навантаження на підтримку міток безпеки, що призводить до повільніших і трудомістких процесів.

Дискреційний контроль доступу (DAC)

Дискреційний контроль доступу (DAC) дозволяє власникам ресурсів приймати рішення щодо безпеки, дозволяючи їм надавати дозволи на ресурси, які вони контролюють. У цьому процесі адміністратор безпеки створює профіль ресурсу з детальним описом дозволів доступу через список контролю доступу.

На відміну від обов'язкового контролю доступу, який залежить від однієї особи, DAC дозволяє групам адміністраторів або не-IT-користувачів контролювати доступ. Забезпечуючи суб'єктам максимальну свободу, DAC пропонує нижчий рівень безпеки порівняно з іншими моделями. Параметр спільного використання в більшості операційних систем відображає DAC, дозволяючи користувачам встановлювати привілеї читання/запису та вимоги до пароля для документів, що належать їм, у таблиці окремих осіб і груп користувачів.

Переваги

- Гнучкий і простий: DAC дозволяє власникам ресурсів оперативно додавати нових користувачів і привілеї, не чекаючи централізованого затвердження.
- Гнучкість для бізнесу: оскільки запити на зміну політики не вимагають схвалення адміністраторів безпеки, прийняття рішень стає більш гнучким і узгоджується з вимогами бізнесу.

Недоліки

- Гнучкість може призвести до надмірних або недостатніх привілейованих користувачів.

- Обмежена видимість: адміністраторам безпеки важко контролювати спільне використання ресурсів і їм потрібно шукати в кількох списках керування доступом, щоб переглянути окремі привілеї.
- Розсуд користувача DAC може створити невідповідності та прогалини в нагляді, створюючи ризики для безпеки.

Потребує постійного спостереження і спостереження.

Контроль доступу на основі ролей (RBAC)

Контроль доступу на основі ролей (RBAC) призначає привілеї доступу відповідно до посадових ролей користувачів. Ця модель є звичайним компонентом систем контролю доступу, які використовуються в промислових системах управління (ICS). На відміну від обов'язкового та дискреційного контролю доступу, RBAC спрощує керування IT-привілеями за допомогою автоматизації. Він групує користувачів у ролі на основі відділу та посади з відповідними ролями дозволів, адаптованими до вимог доступу кожної групи. Це спрощує процес надання відповідних дозволів новим користувачам після входу.

Переваги

- Автоматизований і масштабований.
- Простота в обслуговуванні: робить ефективними завдання з підключення та виключення користувачів із налаштування ролей.
- Централізовані політики в організації.
- Менший ризик: доступ користувачів до ресурсів узгоджується з їхніми ролями, що зменшує потенційні ризики для безпеки.

Недоліки

- Комплексне розгортання у великих організаціях.
- Менші ролі підвищують безпеку, але можуть призвести до збігів.

Призначення занадто великої кількості ролей може призвести до непотрібних привілеїв.

Контроль доступу на основі правил (RuBAC)

Для визначення доступу до об'єктів RuBAC використовує запрограмовані умови, встановлені адміністратором. На відміну від деяких моделей, RuBAC враховує не лише суб'єкт і об'єкт, а й дію, подібно операторам if-then у кодуванні. Він може

вмістити кілька умов і змінних для рішень щодо доступу. Організаціям, які потребують обмеження доступу на основі часу або місця розташування, RuBAC може бути корисним, але зміна запрограмованих умов вимагає часу та досвіду кодування [3].

Zero Trust

Архітектура нульової довіри — це стратегія кібербезпеки, яка працює за простим, але потужним принципом: «Ніколи не довіряй, завжди перевіряй». На відміну від традиційних моделей безпеки, які зосереджуються лише на захисті периметра, нульова довіра передбачає, що загрози можуть надходити з будь-якого місця, як ззовні, так і всередині мережі. Цей підхід розглядає кожен запит доступу до мережі як потенційну загрозу, яка потребує перевірки незалежно від того, звідки він походить. Йдеться про те, щоб лише потрібні люди з належним рівнем доступу могли отримати доступ до цінних даних, і їх щоразу перевіряли.

В основі стратегії нульової довіри лежить віра в те, що організації вже піддаються атаці або можуть піддатися атаці в будь-який момент. Таке мислення змінює спосіб застосування заходів безпеки, гарантуючи, що кожен запит на доступ до мережі досліджується та автентифікується. Прийнявши нульову довіру, компанії встановлюють динамічний і гнучкий захист, який пристосовується до появи нових загроз і зміни потреб організації. Це робить мережу більш стійкою до атак, оскільки мінімізує ймовірність того, що зловмисники проскочать крізь неї непоміченими. По суті, нульова довіра означає захист цифрових активів шляхом припущення, що мережа завжди під загрозою, і дій відповідно [4].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЇ НА БАЗІ ТЕХНОЛОГІЇ ZERO TRUST

2.1. Концепція Zero Trust: основи, принципи та ключові особливості

Перехід від традиційної архітектури безпеки мережі до архітектури нульової довіри знаменує значну еволюцію в тому, як організації захищають свої цифрові активи. Традиційні моделі безпеки ґрунтуються на припущенні, що можна довіряти всьому всередині мережі організації, зосереджуючись на захисті периметра від зовнішніх загроз. Цей підхід «довіряй, але перевіряй» став менш ефективним, оскільки кіберзагрози стали більш витонченими, а внутрішні зломи більш поширеними. Навпаки, архітектура нульової довіри працює за принципом «ніколи не довіряй, завжди перевіряй», обробляючи кожен запит доступу так, ніби він походить із ненадійної мережі. Ця перспектива вимагає суворої перевірки кожного користувача та пристрою, які намагаються отримати доступ до ресурсів, незалежно від їхнього розташування відносно периметра мережі.

Архітектура безпеки з нульовою довірою пропонує більш адаптивний і динамічний метод захисту цифрових переваг організації. Вимагаючи постійної перевірки облікових даних і використовуючи доступ з найменшими привілеями, він мінімізує поверхню атаки та зменшує ймовірність несанкціонованого доступу. Мережна архітектура з нульовою довірою підвищує безпеку даних і програм і дозволяє організаціям бути більш гнучкими, забезпечуючи безпечний доступ для віддалених співробітників і сторонніх співробітників. Принципи нульової довіри однаково застосовуються для всіх користувачів і пристроїв, що забезпечує послідовні заходи безпеки. Крім того, він відіграє вирішальну роль у запобіганні DDoS-атакам шляхом сегментації доступу до мережі та суворої перевірки трафіку. Крім того, прийняття принципів нульової довіри захищає мережі від складних кіберзагроз, таких як соціальна інженерія. Таким чином, він забезпечує надійну структуру, яка може швидко адаптуватися до нових загроз і змін в IT-середовищі.

Основні принципи архітектури нульової довіри

Визначення архітектури базується на простому, але потужному принципі: нікому не довіряти, перевіряти всіх. Цей підхід зміщує фокус безпеки з традиційного захисту на основі периметра на більш комплексну модель, яка розглядає кожен запит доступу так, ніби він надходить із ненадійної мережі. Девіз «ніколи не довіряй, завжди перевіряй» формує цей спосіб мислення, змушуючи організації автентифікувати та авторизувати кожного користувача та пристрій перед наданням доступу до ресурсів, незалежно від їхнього розташування в мережі організації чи за її межами.

Ядро архітектури нульової довіри побудовано на трьох основних концепціях:

Явно перевіряйте: кожен запит на доступ, як від особи, так і від пристрою, має пройти сувору автентифікацію, авторизацію та постійну перевірку конфігурації та стану безпеки, перш ніж отримати доступ до ресурсів.

Використовуйте найменш привілейований доступ: ця концепція обмежує доступ користувачів за допомогою принципів достатнього доступу (JEA) і своєчасного (JIT), зменшуючи поверхню атаки, надаючи користувачам лише той доступ, який їм потрібен для виконання завдань, і нічого більше.

Припустити порушення: працюючи на основі припущення, що порушення можуть і будуть відбуватися, цей принцип зосереджується на мінімізації впливу порушення шляхом сегментації доступу, обмеження бокового руху в мережі та посилення моніторингу ненормальної активності.

Надійна архітектура нульової довіри значною мірою сприяє управлінню IT-ризиками, проактивно виявляючи й пом’якшуючи потенційні загрози безпеці, перш ніж вони вплинуть на мережу. Він узгоджується з принципом «припустити порушення» та постійно перевіряє кожен запит на доступ.

Сім стовпів архітектури нульової довіри

У світі архітектури нульової довіри структура побудована на семи основних стовпах, які забезпечують її ефективність і надійність. Ці стовпи служать керівними принципами для створення безпечної мережі, яка не покладається лише на традиційний захист периметра.

Перевірка особи користувача: кожен користувач, який отримує доступ до системи, повинен бути авторизований. Цей стовп підкреслює важливість надійних процесів перевірки особи, таких як багатофакторна автентифікація (MFA), щоб гарантувати, що доступ надається лише перевіреним користувачам.

Безпека пристрою: гарантує, що всі пристрої, які отримують доступ до мережі, безпечні та відповідають політикам безпеки організації. Це передбачає оновлення пристроїв за допомогою останніх виправлень безпеки та використання рішень керування мобільними пристроями (MDM) для керування безпекою пристрою.

Сегментація мережі: це передбачає поділ мережі на менші керовані сегменти. Сегментація допомагає ефективніше контролювати доступ і обмежувати поширення загроз у мережі.

Захист даних: фокусується на шифруванні даних як у стані спокою, так і під час передачі. Цей стовп гарантує, що конфіденційна інформація завжди захищена, незалежно від її розташування.

Моніторинг і реагування: важливий постійний моніторинг мережевої діяльності. Це дозволяє швидко виявляти підозрілу поведінку та негайно реагувати на потенційні загрози.

Політики безпеки: це правила та політики, які регулюють доступ до мережі та її використання. Політики мають бути динамічними, адаптуватися до змін у ландшафті загроз і потреб організації.

Найменший привілейований доступ: користувачам і пристроям надається лише мінімальний рівень доступу, необхідний для виконання їхніх завдань. Цей принцип зменшує ризик витоку даних, обмежуючи доступ до конфіденційної інформації.

Кожен із цих стовпів відіграє вирішальну роль в архітектурі нульової довіри, забезпечуючи безпеку кожного аспекту мережі. Дотримуючись цих принципів, організації можуть створити більш стійку та чутливу систему безпеки, яка краще готова долати виклики сучасного цифрового світу.

Переваги та проблеми архітектури нульової довіри

Прийняття архітектури нульової довіри дає кілька ключових переваг, усі спрямовані на посилення захисту організації від кіберзагроз. По суті, нульова довіра підвищує рівень безпеки, наполягаючи на суворій перевірці кожного запиту на

доступ, незалежно від походження. Цей підхід «ніколи не довіряй, завжди перевіряй» значно мінімізує ймовірність несанкціонованого доступу, різко знижуючи ризик витоку даних. Покращена безпека полягає не лише у запобіганні несанкціонованому доступу; це також забезпечує точний контроль над тим, хто має доступ до чого у мережі, гарантуючи, що користувачі та пристрої мають лише необхідні дозволи, таким чином дотримуючись принципу найменших привілеїв. Впровадження архітектури нульової довіри покращує методи керування вразливістю, забезпечуючи безперервне сканування та виправлення вразливостей у всіх точках доступу до мережі. Ці переваги разом створюють більш безпечне, стійке та надійне IT-середовище.

Однак перехід до архітектури нульової довіри не позбавлений перешкод. Перехід може бути складним і вимагає детального розуміння поточної мережі та налаштувань безпеки організації. Реалізація нульової довіри часто передбачає капітальний перегляд існуючих політик безпеки та інфраструктури, що може бути трудомістким і дорогим. Крім того, складність налаштування архітектури нульової довіри може вимагати додаткового навчання IT-персоналу, що посилить проблеми впровадження. Хоча ці перешкоди значні, вони не є неможливими. Завдяки ретельному плануванню, чіткій стратегії та правильних інструментів організації можуть впоратися з цими проблемами та отримати значні переваги безпеки, які пропонує архітектура нульової довіри. Примітний приклад архітектури нульової довіри можна побачити у випадку фірми, що надає фінансові послуги, яка перебудувала безпеку своєї мережі, реалізувавши модель нульової довіри. Цей підхід передбачав розгортання програмних рішень з нульовою довірою в цифровому середовищі, що призвело до значного зменшення випадків порушення даних і спроб несанкціонованого доступу.

Архітектура нульової довіри – це не просто тенденція; це життєво важлива система безпеки, яка підходить для широкого кола організацій і секторів. Незалежно від того, керуєте ви невеликим стартапом чи керуєте великим підприємством, принципи нульової довіри можуть значно підвищити рівень кібербезпеки. Цей підхід особливо корисний для секторів, які обробляють конфіденційні дані, як-от фінансові послуги, охорона здоров’я та державні установи, де ймовірність витоку даних

неймовірно висока. Ці сектори можуть використовувати нульову довіру для захисту від складних кіберзагроз, забезпечуючи доступ лише автентифікованих і авторизованих користувачів до критично важливих систем і даних.

Однак привабливість архітектури нульової довіри виходить далеко за межі цих секторів з високими ставками. У сучасному цифровому світі навіть малі підприємства не захищені від кіберзагроз. Універсальна застосовність Zero trust означає, що він є настільки ж важливим для цих невеликих організацій, забезпечуючи масштабований і гнучкий підхід до безпеки, який росте разом із бізнесом. Принадність нульової довіри полягає в її адаптивності — незалежно від розміру організації, галузі чи характеру її даних. Запровадження принципів нульової довіри може значно посилити його механізми захисту від кіберзагроз, що постійно змінюються. Цей інклюзивний підхід гарантує, що кожна організація зможе досягти надійної безпеки. Це робить архітектуру нульової довіри розумним вибором для будь-якої організації, яка цінує цілісність і захист своїх цифрових ресурсів.

Вибір правильної платформи Zero Trust

Вибираючи правильну платформу нульової довіри для організації, дуже важливо зосередитися на функціях, які відповідають основним принципам архітектури нульової довіри. Платформа має пропонувати надійну перевірку особи, забезпечити найменш привілейований доступ і забезпечити мікросегментацію для безпечного керування та моніторингу трафіку у мережі. Ось основні аспекти, які слід враховувати:

Перевірка ідентифікації та контроль доступу: виберіть платформу, яка забезпечує надійне керування ідентифікацією та доступом (IAM). Він має підтримувати багатофакторну автентифікацію (MFA) і динамічне формування політики на основі контексту користувача, пристрою та програми. Це гарантує, що лише автентифіковані та авторизовані користувачі та пристрої зможуть отримати доступ до мережі та ресурсів.

Можливості мікросегментації: шукайте платформи, які пропонують мікросегментацію, що дозволяє розділити мережу на безпечні зони. Ця функція допомагає контролювати доступ до конфіденційних даних і систем, обмежуючи потенційний вплив злому. Ефективна мікросегментація підтримує детальне

застосування політик безпеки, що ускладнює зловмисникам пересування по всій мережі.

Прозорість і аналітика: ефективна платформа нульової довіри повинна забезпечувати повну видимість мережевого трафіку та аналітику в реальному часі. Це дає змогу виявляти підозрілу діяльність і потенційні загрози, забезпечуючи швидке реагування та дії з усунення несправностей. Видимість у всіх мережевих і хмарних середовищах є важливою для підтримки ефективної позиції нульової довіри.

Крім того, при оцінці платформ з нульовою довірою важливо враховувати роль програмного забезпечення з нульовою довірою. Це програмне забезпечення є основою моделі нульової довіри, пропонуючи функції, які мають вирішальне значення для дотримання принципу «ніколи не довіряй, завжди перевіряй».

У цю цифрову еру використання архітектури нульової довіри стає важливим кроком для досягнення підвищеної безпеки мережі. Детальні процеси перевірки цього підходу та акцент на найменших привілеях гарантують, що дані організації залишатимуться захищеними від кіберзагроз, що постійно розвиваються. Інтеграція керування мобільними пристроями (MDM) із принципами нульової довіри ще більше підвищує безпеку, забезпечуючи повний нагляд і контроль над кожним пристроєм у мережі [4].

2.2. Архітектура Zero Trust в інформаційному середовищі

Є багато логічних компонентів, які складають розгортання ZTA в організації. Ці компоненти можуть працювати як локальна служба або через хмарну службу. Модель концептуальної основи на рис.2.1. показує базовий зв’язок між компонентами та їх взаємодією. Зверніть увагу, що це ідеальна модель, яка показує логічні компоненти та їх взаємодію. На рис.2.1. точка прийняття рішень (PDP) розбивається на два логічні компоненти: механізм політики та адміністратор політики (визначено нижче). Логічні компоненти ZTA використовують окрему площину керування для зв’язку, тоді як дані програми передаються на площині даних.

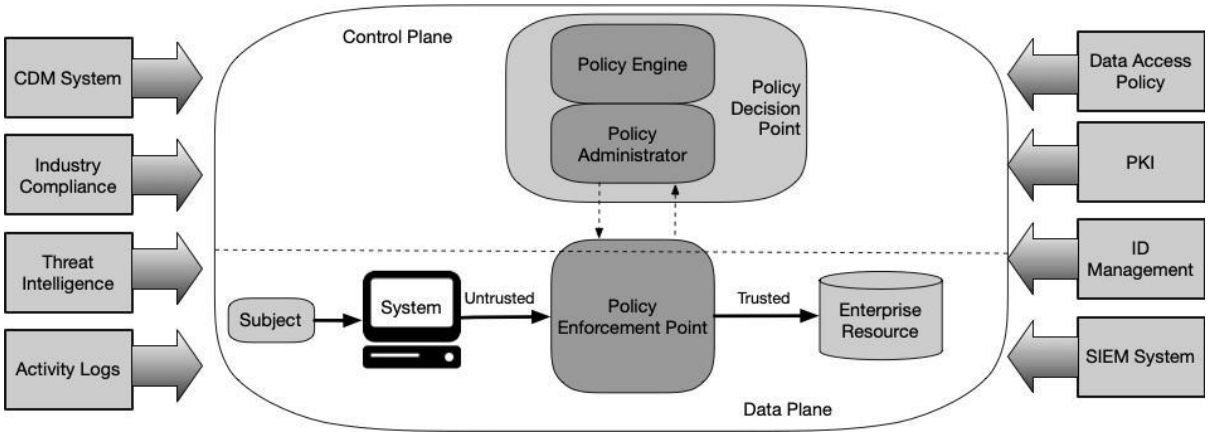

Рис. 2.1. Логічні компоненти Core Zero Trust

Опис компонентів:

• Механізм політики (PE): Цей компонент відповідає за остаточне рішення про надання доступу до ресурсу для певного предмета. PE використовує політику підприємства, а також дані із зовнішніх джерел (наприклад, системи CDM, служби аналізу загроз, описані нижче) як вхідні дані для алгоритму довіри, щоб надати, заборонити або скасувати доступ до ресурсу. PE поєднується з компонентом адміністратора політики. Механізм політики приймає та реєструє рішення (як ухвалене чи відхилене), а адміністратор політики виконує це рішення.

• Адміністратор політики (PA): Цей компонент відповідає за встановлення та/або закриття шляху зв’язку між суб’єктом і ресурсом (через команди для відповідних PEP). Він генерував би будь-яку спеціальну автентифікацію для сеансу та маркер автентифікації або облікові дані, які 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 PEP, щоб дозволити розпочати сеанс. Якщо сеанс відхилено (або попереднє схвалення відхилено), PA сигналізує PEP закрити з’єднання. Деякі реалізації можуть розглядати PE та PA як одну послугу; тут вона поділяється на її дві логічні складові. PA зв’язується з PEP під час створення шляху зв’язку. Цей зв'язок здійснюється через площину керування.

• Пункт контролю за дотриманням політики (PEP): Ця система відповідає за активацію, моніторинг і остаточне припинення зв’язків між суб’єктом і корпоративним ресурсом. PEP спілкується з PA, щоб пересилати запити та/або

отримувати оновлення політики від PA. Це єдиний логічний компонент у ZTA, але його можна розбити на два різні компоненти: клієнт (наприклад, агент на ноутбуці) і сторона ресурсу (наприклад, компонент шлюзу перед ресурсом, який контролює доступ) або один компонент порталу, який діє як воротар для шляхів зв’язку. За PEP знаходиться зона довіри розміщення корпоративного ресурсу.

На додаток до основних компонентів на підприємстві, що реалізує ZTA, кілька джерел даних надають правила введення та політики, які використовуються механізмом політики під час прийняття рішень щодо доступу. До них належать локальні джерела даних, а також зовнішні (тобто неконтрольовані компанією або створені нею) джерела даних. Вони можуть включати:

- Система постійної діагностики та пом'якшення (CDM): Збирає інформацію про поточний стан активу підприємства та оновлює конфігурацію та компоненти програмного забезпечення. Корпоративна система CDM надає механізму політики інформацію про актив, який надсилає запит на доступ, наприклад, чи працює на ньому відповідна виправлена операційна система (ОС), цілісність схвалених підприємством програмних компонентів або наявність несхвалених компонентів і чи має актив будь-які відомі вразливості. Системи CDM також відповідають за ідентифікацію та потенційне застосування підмножини політик на некорпоративних пристроях, активних в інфраструктурі підприємства.
- Система відповідності галузі: Гарантує, що підприємство залишається сумісним з будь-яким нормативним режимом, під який воно може потрапити (наприклад, FISMA, вимоги щодо безпеки інформації в галузі охорони здоров’я чи фінансової галузі). Це включає в себе всі правила політики, які підприємство розробляє для забезпечення відповідності.
- Канал(и) даних про загрози: Надає інформацію з внутрішніх або зовнішніх джерел, яка допомагає механізму політики приймати рішення щодо доступу. Це можуть бути кілька служб, які отримують дані з внутрішніх і/або кількох зовнішніх джерел і надають інформацію про нещодавно виявлені атаки чи вразливості. Це також включає нещодавно виявлені недоліки в програмному забезпеченні, нещодавно виявлені зловмисне програмне забезпечення та

зареєстровані атаки на інші активи, до яких механізм політики захоче заборонити доступ із корпоративних активів.

- Журнали мережевої та системної активності: Ця корпоративна система агрегує журнали активів, мережевий трафік, дії доступу до ресурсів та інші події, які забезпечують зворотний зв'язок у режимі реального часу (або майже в реальному часі) щодо безпеки інформаційних систем підприємства.
- Правила доступу до даних: Це атрибути, правила та політики щодо доступу до ресурсів підприємства. Цей набір правил може бути закодований (через інтерфейс керування) або динамічно створений механізмом політики. Ці політики є відправною точкою для авторизації доступу до ресурсу, оскільки вони надають основні привілеї доступу для облікових записів і програм/служб на підприємстві. Ці політики мають ґрунтуватися на визначених ролях місії та потребах організації.
- Інфраструктура відкритих ключів підприємства (PKI): Ця система відповідає за створення та реєстрацію сертифікатів, виданих підприємством ресурсам, суб'єктам, службам і програмам. Це також включає екосистему глобального центру сертифікації та Федеральну PKI, які можуть бути інтегровані або не інтегровані з PKI підприємства. Це також може бути PKI, який не побудований на основі сертифікатів X.509.
- Система управління ID: Відповідає за створення, зберігання та керування корпоративними обліковими записами користувачів і ідентифікаційними записами (наприклад, сервер протоколу доступу до каталогу (LDAP)). Ця система містить необхідну інформацію про тему (наприклад, ім'я, адресу електронної пошти, сертифікати) та інші характеристики підприємства, такі як роль, атрибути доступу та призначені активи. Ця система часто використовує інші системи (наприклад, PKI) для артефактів, пов'язаних з обліковими записами користувачів. Ця система може бути частиною більшої федеративної спільноти та може включати некорпоративних співробітників або посилання на некорпоративні активи для співпраці.
- Система безпеки інформації та управління подіями (SIEM): Збирає інформацію, орієнтовану на безпеку, для подальшого аналізу. Потім ці дані використовуються для вдосконалення політики та попередження про можливі атаки на активи підприємства.

2.3 Варіанти підходів до архітектури нульової довіри

Є кілька способів, за допомогою яких організація може запровадити ZTA для робочих процесів. Ці підходи відрізняються компонентами, що використовуються, і основним джерелом правил політики для організації. Кожен підхід реалізує всі принципи ZT але може використовувати один або два (або один компонент) як основний драйвер політики. Повне рішення ZT включатиме елементи всіх трьох підходів. Ці підходи включають покращене керування ідентифікацією, логічну мікросегментацію та сегментацію на основі мережі.

Певні підходи більше підходять для одних випадків використання, ніж для інших. Організація, яка хоче розробити ZTA для свого підприємства, може виявити, що обраний нею варіант використання та існуючі політики вказують на один підхід над іншими. Це не означає, що інші підходи не працюватимуть, а скоріше те, що інші підходи можуть бути важчими для реалізації та можуть вимагати більш фундаментальних змін у тому, як підприємство зараз здійснює бізнес-потоки.

ZTA використовує розширене керування ідентифікацією

Розширений підхід до управління ідентифікацією для розробки ZTA використовує ідентифікацію учасників як ключовий компонент створення політики. Якби суб’єкти не запитували доступ до ресурсів підприємства, не було б потреби створювати політики доступу. Для цього підходу політики доступу до корпоративних ресурсів базуються на ідентифікації та призначених атрибутах. Основна вимога до доступу до ресурсу базується на привілеях доступу, наданих даному суб’єкту. Інші фактори, такі як використовуваний пристрій, стан активів і фактори навколишнього середовища, можуть змінити остаточний розрахунок рівня достовірності (і кінцеву авторизацію доступу) або певним чином адаптувати результат, наприклад надання лише часткового доступу до певного джерела даних на основі розташування в мережі. Індивідуальні ресурси або PEP мережевий стек OSI). Ці підходи іноді називають підходами програмно визначеного периметра (SDP) і часто включають концепції програмно визначених мереж (SDN) [SDNBOOK] і мереж на основі намірів (IBN) [IBNVN]. У цьому підході PA діє як мережевий контролер, який налаштовує та

переконфігурує мережу на основі рішень, прийнятих PE. Клієнти продовжують запитувати доступ через PEP, якими керує компонент PA.

Коли цей підхід реалізовано на мережевому рівні програми (тобто на рівні 7), найпоширенішою моделлю розгортання є агент/шлюз. У цій реалізації агент і шлюз ресурсу (діючи як єдиний PEP і налаштований PA) встановлюють безпечний канал, який використовується для зв'язку між клієнтом і ресурсом. Можуть існувати й інші варіанти цієї моделі, а також для хмарних віртуальних мереж, мереж без IP тощо.

Розгорнуті варіації абстрактної архітектури

Усі перераховані вище компоненти є логічними компонентами. Вони 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, PKI, керований підприємством, може складатися з одного компонента, який відповідає за видачу сертифікатів для пристроїв, а інший використовується для видачі сертифікатів кінцевим користувачам, але обидва використовують проміжні сертифікати, видані одним корпоративним центром сертифікації. У деяких пропозиціях продуктів ZT, які зараз доступні на ринку, компоненти PE та PA об'єднані в одній службі.

Існує кілька варіантів розгортання вибраних компонентів архітектури. Залежно від того, як налаштовано мережу підприємства, кілька моделей розгортання ZTA можуть використовуватися для різних бізнес-процесів на одному підприємстві.

Розгортання на основі агента пристрою/шлюзу

У цій моделі розгортання PEP розділений на два компоненти, які знаходяться на ресурсі або як компонент безпосередньо перед ресурсом. Наприклад, кожен ресурс, випущений підприємством, має встановлений агент пристрою, який координує з'єднання, і кожен ресурс має компонент (тобто шлюз), який розміщується безпосередньо попереду, щоб ресурс спілкувався лише зі шлюзом, по суті, слугуючи проксі для ресурс. Агент — це програмний компонент, який спрямовує частину (або весь) трафік до відповідного PEP для оцінки запитів. Шлюз відповідає за зв'язок із адміністратором політики та дозволяє лише схвалені шляхи зв'язку, налаштовані адміністратором політики.

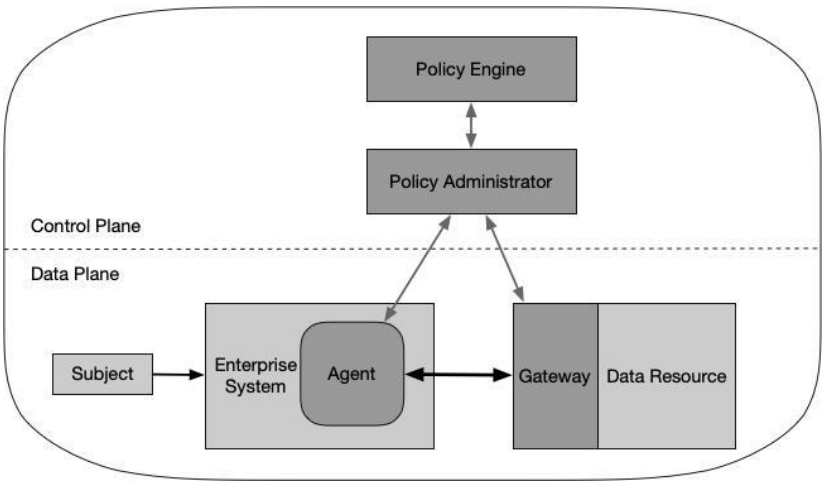

Рис.2.2. Модель агента пристрою/шлюзу

У типовому сценарії суб'єкт із корпоративним портативним комп'ютером бажає під'єднатися до корпоративного ресурсу (наприклад, програми/бази даних кадрових ресурсів). Запит на доступ приймає локальний агент і пересилає запит адміністратору політики. Адміністратор політики та механізм політики можуть бути локальним активом підприємства або хмарною службою. Адміністратор політики пересилає запит механізму політики для оцінки. Якщо запит авторизовано, адміністратор політики налаштовує канал зв'язку між агентом пристрою та відповідним ресурсним шлюзом через площину керування. Це може включати таку інформацію, як адреса Інтернет-протоколу (IP), інформація про порт, ключ сеансу або подібні артефакти безпеки. Потім агент пристрою та шлюз з'єднуються, і починаються потоки зашифрованих даних програми/сервісу. З'єднання між агентом пристрою та шлюзом ресурсів припиняється, коли робочий процес завершено або коли його запускає адміністратор політики через подію безпеки (наприклад, час очікування сеансу, невдача повторної автентифікації).

Цю модель найкраще використовувати для підприємств, які мають надійну програму керування пристроями, а також окремі ресурси, які можуть спілкуватися зі шлюзом. Для підприємств, які активно використовують хмарні сервіси, це клієнт-серверна реалізація програмно-визначеного периметра (SDP) [CSA-SDP] Cloud Security Alliance (CSA). Ця модель також підходить для підприємств, яким не потрібна політика BYOD. Доступ можливий лише через агент пристрою, який можна розмістити на активах підприємства.

Розгортання на основі анклаву

Ця модель розгортання є різновидом моделі агента пристрою/шлюзу вище. У цій моделі компоненти шлюзу можуть розташовуватися не на активах або перед окремими ресурсами, а на межі анклаву ресурсів (наприклад, локального центру обробки даних), як показано на рис.2.3. Зазвичай ці ресурси обслуговують один бізнес-функцією або може не мати змоги зв'язуватися безпосередньо зі шлюзом (наприклад, застаріла система бази даних, яка не має інтерфейсу прикладного програмування [API], який можна використовувати для зв'язку зі шлюзом). Ця модель розгортання також може бути корисною для підприємств, які використовують хмарні мікросервіси для окремих бізнес-процесів (наприклад, сповіщення користувачів, пошук бази даних, виплата зарплати). У цій моделі вся приватна хмара розташована за шлюзом.

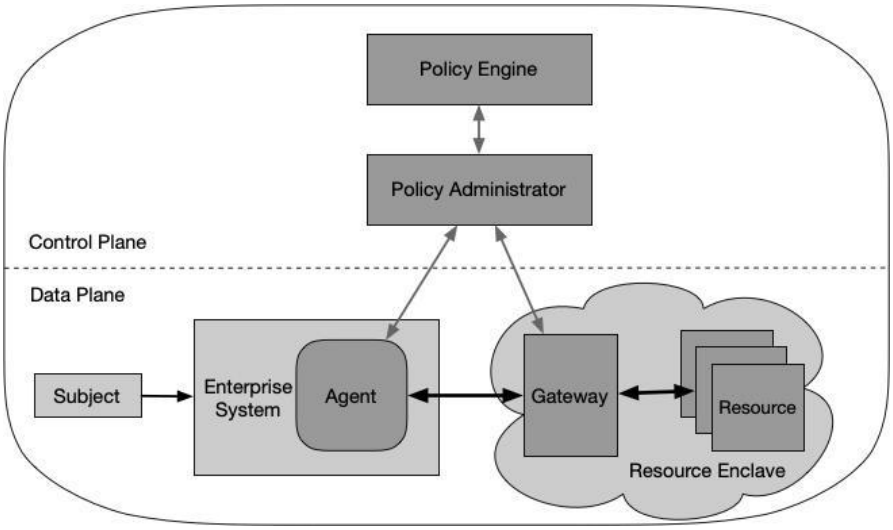

Рис.2.3. Модель анклавного шлюзу

Ця модель може бути гібридом із моделлю агент пристрою/шлюз. У цій моделі корпоративні активи мають агента пристрою, який використовується для підключення до шлюзів анклаву, але ці підключення створюються за допомогою того самого процесу, що й базова модель агента пристрою/шлюзу.

Ця модель корисна для підприємств, які мають застарілі програми або локальні центри обробки даних, які не можуть мати окремі шлюзи. Підприємству потрібна надійна програма керування активами та конфігураціями для встановлення/налаштування агентів пристроїв. Недоліком є те, що шлюз захищає

колекцію ресурсів і може бути не в змозі захистити кожен ресурс окремо. Це також може дозволити суб'єктам переглядати ресурси, на доступ до яких вони не мають привілеїв.

Розгортання на основі порталу ресурсів

У цій моделі розгортання PEP є єдиним компонентом, який діє як шлюз для суб'єктних запитів. Портал шлюзу може бути для окремого ресурсу або безпечним анклавом для набору ресурсів, які використовуються для однієї бізнес-функції. Одним із прикладів може бути портал шлюзу в приватну хмару або центр обробки даних, що містить успадковані програми, як показано на рис.2.4.

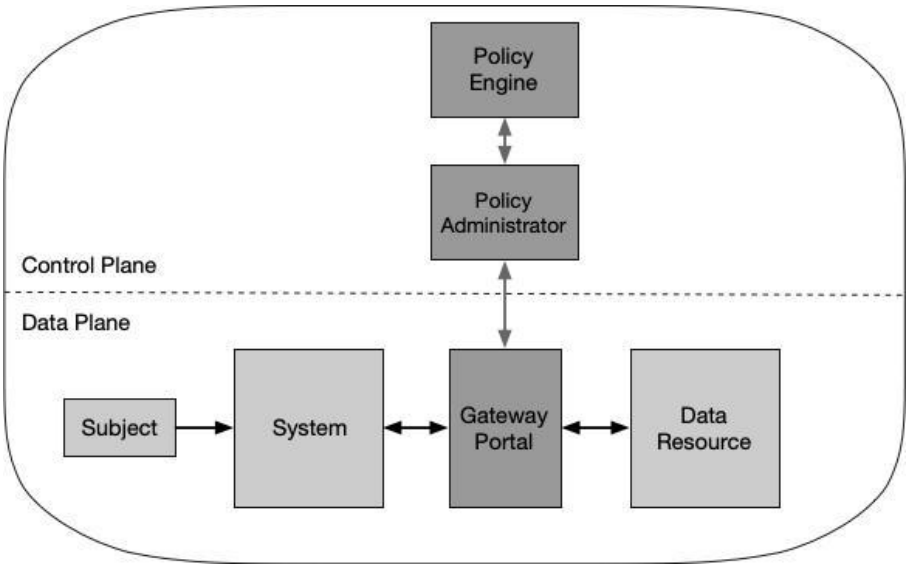

Рис.2.4. Модель порталу ресурсів

Основна перевага цієї моделі перед іншими полягає в тому, що програмний компонент не потрібно встановлювати на всіх клієнтських пристроях. Ця модель також більш гнучка для політик BYOD і проектів міжорганізаційної співпраці. Адміністраторам підприємства не потрібно переконуватися, що кожен пристрій має відповідний агент пристрою перед використанням. Однак із пристроїв, які запитують доступ, можна отримати обмежену інформацію. Ця модель може сканувати та аналізувати активи та пристрої лише після їх підключення до порталу PEP і може бути не в змозі постійно відстежувати їх на наявність зловмисного програмного забезпечення, невиправлених уразливостей і відповідної конфігурації.

Основна відмінність цієї моделі полягає в тому, що немає локального агента, який обробляє запити, і тому підприємство може не мати повної видимості або довільного контролю над активами, оскільки воно може переглядати/сканувати їх, лише коли вони підключаються до порталу. Для пом’якшення або компенсації підприємство може застосувати такі заходи, як ізоляція браузера. Ці активи можуть бути невидимими для підприємства між цими сеансами. Ця модель також дозволяє зловмисникам виявити та спробувати отримати доступ до порталу чи спроби атаки типу "відмова в обслуговуванні" (DoS) проти порталу. Системи порталу повинні бути добре налаштовані, щоб забезпечити доступність проти атаки DoS або збою в роботі мережі.

Ізольоване програмне середовище пристрою

Інший варіант моделі розгортання агента/шлюзу полягає в тому, що перевірені додатки або процеси виконуються розділено на активи. Ці відсіки можуть бути віртуальними машинами, контейнерами чи іншими реалізаціями, але мета та сама: захистити програму або екземпляри програм від можливо скомпрометованого хоста чи інших програм, які працюють на ресурсі.

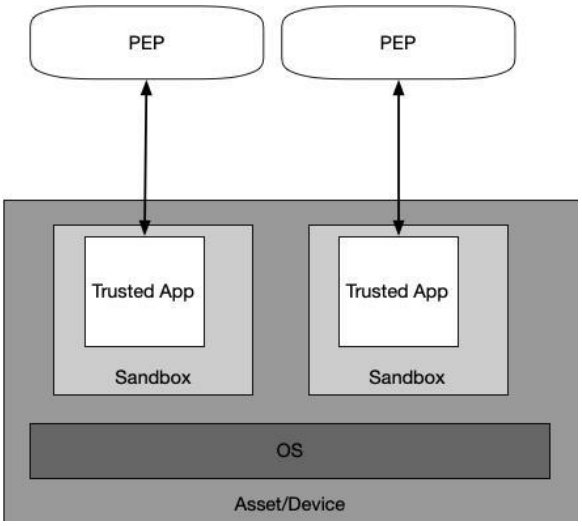

Рис.2.5. Пісочниці програми

На рис.2.5. досліджуваний пристрій запускає схвалені, перевірені програми в пісочниці. Програми можуть зв’язуватися з PEP, щоб отримати доступ до ресурсів, але PEP відхилить запити від інших програм на ресурсі. PEP може бути корпоративною локальною службою або хмарною службою в цій моделі.

Основна перевага цього варіанту моделі полягає в тому, що окремі додатки сегментовані від решти активу. Якщо актив неможливо перевірити на наявність уразливостей, ці окремі програми ізольованого програмного середовища можуть бути захищені від потенційного зараження зловмисним програмним забезпеченням на хост-ресурсі. Одним із недоліків цієї моделі є те, що підприємства повинні підтримувати ці програми ізольованого програмного середовища для всіх активів і можуть не мати повної видимості клієнтських активів. Підприємство також має переконатися, що кожна ізольована програма безпечна, що може вимагати більше зусиль, ніж просто моніторинг пристроїв.

Алгоритм довіри

Для підприємства з розгортанням ZTA механізм політики можна розглядати як мозок, а алгоритм довіри PE — як його основний розумовий процес. Алгоритм довіри (TA) — це процес, який використовується механізмом політики для остаточного надання або заборони доступу до ресурсу. Механізм політики отримує вхідні дані з кількох джерел: база даних політики з доступною для спостереження інформацією про суб'єктів, атрибути та ролі суб'єктів, історичні моделі поведінки суб'єктів, джерела розвідки про загрози та інші джерела метаданих. Процес можна згрупувати в широкі категорії та візуалізувати на рис.2.7.

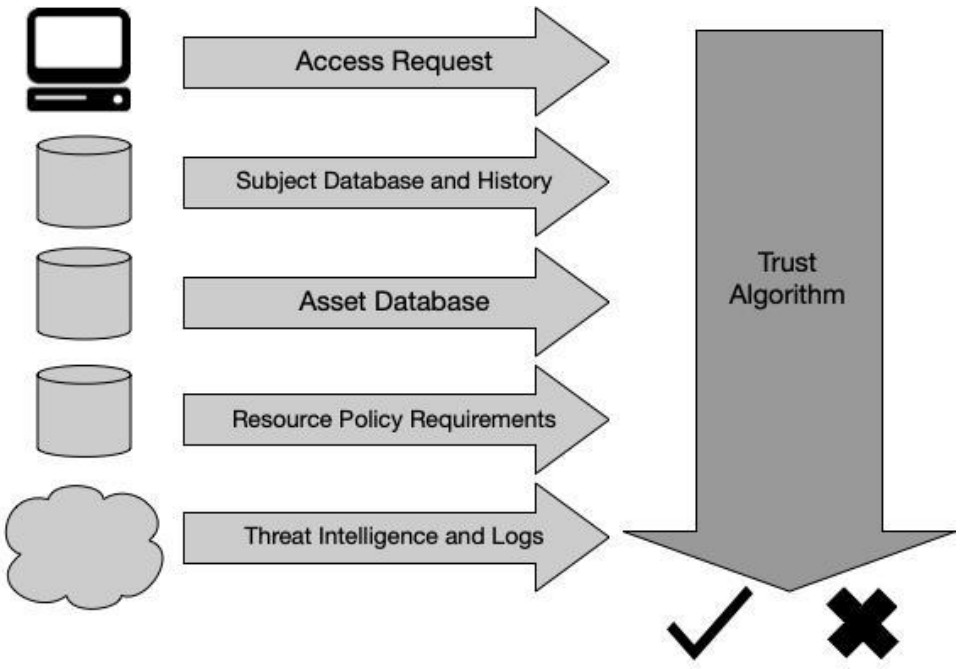

Рис.2.6. Введення алгоритму довіри

На рис.2.6. вхідні дані можна розбити на категорії залежно від того, що вони надають алгоритму довіри.

- Запит на доступ: Це власне запит суб'єкта. Запитуваний ресурс є основною інформацією, але також використовується інформація про запитувача. Це може включати версію ОС, програмне забезпечення, що використовується (наприклад, чи відображається програма, яка запитує, у списку схвалених програм?) і рівень виправлення. Залежно від цих факторів і стану безпеки активів доступ до активів може бути обмежено або заборонено.
- Тематична база даних: Це «хто», який запитує доступ до ресурсу [SP800-63]. Це набір суб’єктів (людей і процесів) підприємства або співавторів і набір призначених суб’єктам атрибутів/привілеїв. Ці суб’єкти та атрибути формують основу політики доступу до ресурсів [SP800-162] [NISTIR 7987]. Ідентифікаційні дані користувача можуть включати комбінацію логічної ідентифікаційної інформації (наприклад, ідентифікатора облікового запису) та результатів перевірок автентифікації, які виконують PEP. Атрибути ідентичності, які можна враховувати при визначенні рівня надійності, включають час і геолокацію. Набір привілеїв, наданих декільком суб’єктам, можна розглядати як роль, але привілеї слід призначати суб’єкту на індивідуальній основі, а не просто тому, що вони можуть відповідати певній ролі в організації. Ця колекція повинна бути закодована та збережена в системі керування ідентифікаторами та базі даних політики. Це також може включати дані про минулу спостережувану поведінку суб’єкта в деяких (TA) варіантах.
- База даних активів (і спостережуваний статус): Це база даних, яка містить відомий статус кожного активу, що належить підприємству (і, можливо, відомого непідприємства/BYOD) (до певної міри фізичного та віртуального). Це порівнюється зі спостережуваним статусом активу, який надсилає запит, і може включати версію ОС, наявне програмне забезпечення та його цілісність, розташування (розташування в мережі та геолокація) і рівень виправлення. Залежно від стану активів у порівнянні з цією базою даних доступ до активів може бути обмежено або заборонено.
- Вимоги до ресурсів: Цей набір політик доповнює ідентифікатор користувача та базу даних атрибутів [SP800-63] і визначає мінімальні вимоги для доступу до ресурсу. Вимоги можуть включати рівні гарантії автентифікатора, такі як

розташування мережі MFA (наприклад, заборона доступу з іноземних IP-адрес), конфіденційність даних і запити на конфігурацію активів. Ці вимоги повинні бути розроблені як зберігачем даних (тобто тими, хто відповідає за дані), так і тими, хто відповідає за бізнес-процеси, які використовують дані (тобто тими, хто відповідає за місію).

- Розвідка загроз: Це інформаційний канал або канали про загальні загрози та активне шкідливе програмне забезпечення, що працює в Інтернеті. Це також може включати конкретну інформацію про зв'язок, який спостерігається з пристрою, який може бути підозрілим (наприклад, запити щодо можливих командних і контрольних вузлів зловмисного програмного забезпечення). Ці канали можуть бути зовнішніми службами або внутрішніми скануваннями та виявленнями, а також можуть містити сигнатури атак і пом'якшення. Це єдиний компонент, який швидше за все буде під контролем служби, а не підприємства.

Вага важливості для кожного джерела даних може бути власним алгоритмом або може бути налаштована підприємством. Ці значення ваги можна використовувати для відображення важливості джерела даних для підприємства.

Остаточне визначення потім передається PA для виконання. Робота PA полягає в тому, щоб налаштувати необхідні PEP, щоб дозволити авторизоване спілкування. Залежно від того, як розгортається ZTA, це може включати надсилання результатів автентифікації та інформації про конфігурацію підключення до шлюзів і агентів або порталів ресурсів. PA також можуть затримати або призупинити сеанс зв'язку, щоб повторно автентифікувати та повторно авторизувати з'єднання відповідно до вимог політики. PA також відповідає за видачу команди для припинення з'єднання на основі політики (наприклад, після тайм-ауту, коли робочий процес завершено, через попередження безпеки).

Варіації алгоритму довіри

Існують різні способи реалізації TA. Різні реалізатори можуть побажати по-різному зважити наведені вище фактори відповідно до сприйнятої важливості факторів. Є ще дві основні характеристики, які можна використовувати для диференціації TA. По-перше, як оцінюються фактори, чи то як двійкові рішення, чи як зважені частини цілого «балу» чи рівня довіри. По-друге, як запити оцінюються по

відношенню до інших запитів тим самим суб’єктом, програмою/сервісом або пристроєм.

• Критерії проти балів: ТА на основі критеріїв передбачає набір кваліфікованих атрибутів, які повинні бути виконані перед тим, як буде надано доступ до ресурсу або буде дозволено дію (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 балів обчислює рівень достовірності 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).

• Сингуляр проти контекстуального: Окремий ТА обробляє кожен запит окремо і не бере до уваги історію предмета під час оцінки. Це може дозволити швидше оцінювати, але існує ризик того, що атака може залишитися непоміченою, якщо вона залишиться в межах дозволеної ролі суб’єкта. Контекстний ТА бере до уваги нещодавню історію суб’єкта або мережевого агента під час оцінювання запитів на доступ. Це означає, що PE має підтримувати певну інформацію про стан усіх суб’єктів і програм, але з більшою ймовірністю виявить зловмисника, який використовує підроблені облікові дані для доступу до інформації за шаблоном, який є нетиповим для того, що PE бачить для даного суб’єкта. Це також означає, що PE повинен бути поінформований про поведінку користувача від PA (і PEP), з якими суб’єкти взаємодіють під час спілкування. 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 на ресурси.

Ці два фактори не завжди залежать один від одного. Можна мати ТА, який призначає рівень достовірності для кожного суб’єкта та/або пристрою та все ще розглядає кожен запит доступу незалежно (тобто окремий). Однак контекстні ТА, засновані на балах, нададуть можливість запропонувати більш динамічний і

детальний контроль доступу, оскільки оцінка забезпечує поточний рівень надійності для облікового запису, який запитує, і адаптується до мінливих факторів швидше, ніж статичні політики, змінені адміністраторами.

В ідеалі алгоритм довіри ZTA повинен бути контекстним, але це не завжди можливо з компонентами інфраструктури, доступними для підприємства. Контекстний ТА може пом'якшити загрози, коли зловмисник залишається близьким до «нормального» набору запитів на доступ до скомпрометованого облікового запису або внутрішньої атаки. При визначенні та впровадженні алгоритмів довіри важливо збалансувати безпеку, зручність використання та економічну ефективність. Постійне спонукання суб'єкта повторної автентифікації проти поведінки, яка відповідає історичним тенденціям і нормам для його місійної функції та ролі в організації, може призвести до проблем із зручністю використання. Наприклад, якщо працівник відділу кадрів агентства зазвичай отримує доступ до 20–30 записів співробітників протягом типового робочого дня, контекстний ТА може надіслати сповіщення, якщо кількість запитів на доступ раптово перевищить 100 записів за день. Контекстний ТА також може надіслати сповіщення, якщо хтось надсилає запити на доступ після звичайних робочих годин, оскільки це може бути зловмисник, який викрадає записи за допомогою скомпрометованого облікового запису HR. Це приклади, коли контекстна ТА може виявити атаку, тоді як окрема ТА може не виявити нову поведінку. В іншому прикладі бухгалтер, який зазвичай отримує доступ до фінансової системи в звичайний робочий час, тепер намагається отримати доступ до системи посеред ночі з невпізнаного місця.

Розробка набору критеріїв або ваг/порогових значень для кожного ресурсу потребує планування та тестування. Під час початкового впровадження ZTA адміністратори підприємства можуть зіткнутися з проблемами, коли запити на доступ, які мають бути затверджені, відхиляються через неправильну конфігурацію. Це призведе до початкової фази «налаштування» розгортання. Можливо, знадобиться відкоригувати критерії або ваги оцінки, щоб гарантувати дотримання політик, водночас дозволяючи функціонувати бізнес-процесам підприємства. Тривалість цієї фази налаштування залежить від показників, визначених підприємством для прогресу

та толерантності до неправильних відмов/схвалень доступу до ресурсів, що використовуються в робочому процесі.

Компоненти мережі/оточення

У середовищі ZT має бути відокремлення (логічне або, можливо, фізичне) комунікаційних потоків, які використовуються для керування та налаштування мережі та комунікаційних потоків додатків/служб, які використовуються для виконання фактичної роботи організації. Це часто розбивається на площину керування для зв'язку керування мережею та площину даних для потоків зв'язку програми/сервісу.

Площина керування використовується різними компонентами інфраструктури (як корпоративними, так і постачальниками послуг) для обслуговування та налаштування активів; судити, надавати чи відмовляти в доступі до ресурсів; і виконувати будь-які необхідні операції для встановлення шляхів зв'язку між ресурсами. Площина даних використовується для фактичного зв'язку між програмними компонентами. Цей канал зв'язку може бути неможливим, поки шлях не буде встановлено через площину керування. Наприклад, рівень керування може використовуватися PA та PEP для встановлення шляху зв'язку між суб'єктом і ресурсом підприємства. Тоді робоче навантаження програми/служби використовуватиме встановлений шлях площини даних.

Вимоги до мережі для підтримки ZTA

1. Активи підприємства мають базове підключення до мережі. Локальна мережа (LAN), контрольована підприємством чи ні, забезпечує базову маршрутизацію та інфраструктуру (наприклад, DNS). Віддалений корпоративний актив не обов'язково може використовувати всі служби інфраструктури.

2. Підприємство має мати можливість розрізнити, якими активами володіє або керує підприємство, і поточним станом безпеки пристроїв. Це визначається обліковими даними, виданими підприємством, і не використовує інформацію, яку неможливо автентифікувати (наприклад, MAC-адреси мережі, які можна підробити).

3. Підприємство може спостерігати за всім мережевим трафіком. Підприємство записує пакети, які бачать у площині даних, навіть якщо воно не в змозі виконати інспекцію прикладного рівня (тобто рівня OSI 7) для всіх пакетів.

Підприємство відфільтровує метадані про з’єднання (наприклад, призначення, час, ідентифікатор пристрою), щоб динамічно оновлювати політики та інформувати PE під час оцінки запитів на доступ.

4. Ресурси підприємства не повинні бути доступні без доступу до PEP. Корпоративні ресурси не приймають довільні вхідні підключення з Інтернету. Ресурси приймають спеціально налаштовані підключення лише після того, як клієнт пройшов автентифікацію та авторизацію. Ці шляхи спілкування встановлюються PEP. Ресурси можуть бути навіть недоступні без доступу до PEP. Це не дозволяє зловмисникам ідентифікувати цілі за допомогою сканування та/або запуску DoS-атак на ресурси, розташовані за PEP. Зауважте, що не всі ресурси слід приховувати таким чином; деякі компоненти мережевої інфраструктури (наприклад, сервери DNS) повинні бути доступні.

5. Площина даних і площина керування логічно розділені. Механізм політики, адміністратор політики та PEP спілкуються в мережі, яка логічно відокремлена та недоступна для активів і ресурсів підприємства. Площина даних використовується для трафік даних додатків/служб. Механізм політики, адміністратор політики та PEP використовують площину керування для зв’язку та керування шляхами зв’язку між активами. PEPs повинні мати можливість надсилати та отримувати повідомлення як з площини даних, так і з рівня керування.

6. Активи підприємства можуть досягати компонента PEP. Суб’єкти підприємства повинні мати доступ до компоненту PEP, щоб отримати доступ до ресурсів. Це може мати форму веб-порталу, мережевого пристрою або програмного агента на ресурсі підприємства, який забезпечує підключення.

7. PEP є єдиним компонентом, який отримує доступ до адміністратора політики як частини бізнес-потоку. Кожен PEP, що працює в корпоративній мережі, має з’єднання з адміністратором політики для встановлення шляхів зв’язку від клієнтів до ресурсів. Весь трафік бізнес-процесів підприємства проходить через одного або кількох PEP.

8. Віддалені корпоративні активи повинні мати доступ до корпоративних ресурсів без необхідності попереднього проходження корпоративної мережевої інфраструктури. Наприклад, від віддаленого суб’єкта не слід вимагати використання

зворотного зв’язку з корпоративною мережею (тобто віртуальною приватною мережею [VPN]) для доступу до послуг, що використовуються підприємством і розміщені постачальником загальнодоступної хмари (наприклад, електронна пошта).

9. Інфраструктура, яка використовується для підтримки процесу прийняття рішення про доступ до ZTA, повинна бути масштабованою з урахуванням змін у навантаженні процесу. PE(s), PA(s) і PEPs, що використовуються в ZTA, стають ключовими компонентами будь-якого бізнес-процесу. Затримка або неможливість досягти PEP (або нездатність PEP досягти PA/PE) негативно впливає на здатність виконувати робочий процес. Підприємство, яке впроваджує ZTA, має надати компоненти для очікуваного робочого навантаження або мати можливість швидко масштабувати інфраструктуру, щоб за потреби справлятися з підвищеним використанням.

10. Активи підприємства можуть бути не в змозі охопити певних публічних діячів через політику або спостережувані фактори. Наприклад, може існувати політика, згідно з якою мобільні активи можуть не мати доступу до певних ресурсів, якщо актив, який запитує, знаходиться за межами країни походження підприємства. Ці фактори можуть залежати від розташування (геолокації чи розташування в мережі), типу пристрою чи інших критеріїв [5].

2.4. Аналіз існуючих технологій та інструментів Zero Trust

У сфері кібербезпеки підхід Zero Trust Security розглядається як один із найефективніших, оскільки він виключає концепцію довіри. Модель Zero Trust Security використовує служби ідентифікації для захисту доступу користувачів до програмного забезпечення та інфраструктури, виходячи з припущення, що ненадійні суб’єкти можуть існувати як у межах мережі, так і за її межами.

Розглядаються п’ять ключових практик впровадження Zero Trust Security в організаціях:

Багатофакторна автентифікація (MFA).

Рекомендується застосування багатофакторної автентифікації для додаткової перевірки користувачів. Оскільки використання лише паролів є недостатнім для

сучасних умов, облікові дані користувачів можуть бути доповнені різними факторами автентифікації: тим, що користувач знає, має або чим є. Така перевірка має охоплювати всіх користувачів, включаючи кінцевих і привілейованих користувачів, а також партнерів і клієнтів. Додаткові рівні автентифікації є обов'язковими для доступу до конфіденційних даних або підвищення привілеїв.

Перевірка пристроїв.

Кожен пристрій, що використовується для доступу до корпоративних ресурсів, має бути зареєстрований і перевірений. Контроль ідентифікації повинен поширюватися на кінцеві точки. Використання систем керування мобільними пристроями забезпечує автоматичну реєстрацію сертифікатів і зменшує адміністративні витрати.

Забезпечення відповідності пристроїв політикам безпеки.

Пристрої мають відповідати корпоративним вимогам, таким як шифрування диска, актуальність антивірусного програмного забезпечення та оновлення. Повинен бути передбачений механізм контролю стану пристроїв і управління політиками доступу залежно від ролей або груп користувачів. Необхідно забезпечити автоматичне видалення облікових даних пристроїв у разі їх втрати або зупинення облікових записів користувачів.

Принцип найменших привілеїв.

Доступ до ресурсів має надаватися виключно в межах виконання службових обов'язків. Права адміністратора повинні контролюватися, а доступ до інфраструктури суворо обмежуватися. Цей принцип стосується як привілейованих, так і звичайних користувачів.

Використання адаптивних рішень.

Інноваційні системи керування ідентифікацією використовують машинне навчання для аналізу поведінки користувачів, пристроїв і програм. Наприклад, розпізнавання незвичних дій (доступ до ресурсів із нетипових місць) дозволяє динамічно приймати рішення щодо доступу та привілеїв на основі ризиків.

Дотримання цих практик забезпечує високий рівень захисту корпоративних систем відповідно до концепції Zero Trust.

Xage Zero Trust Access розкриває потенціал для промислових підприємств, забезпечуючи швидшу реакцію на інциденти та більш раціональну співпрацю між партнерами, постачальниками та іншими третіми сторонами. Ці переваги віддаленого доступу не повинні відбуватися за рахунок некерованого ризику. Кібератаки постійно використовують інструменти віддаленого доступу, щоб зламати, викрасти дані та поширювати зловмисне програмне забезпечення. Інструменти віддаленого доступу повинні бути розроблені таким чином, щоб запобігти цьому [6].

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЇ НА БАЗІ ТЕХНОЛОГІЇ ZERO TRUST

3.1. Розгортання архітектури Zero Trust на базі рішення Xage

Традиційні підходи до безпеки та контролю доступу використовують підприємство як периметр, розділяючи активи на зони довіри та автоматично довіряючи та надаючи дозволи машинам, програмам і користувачам у цих зонах довіри. Ці довірчі зони можуть містити тисячі пристроїв із широким спектром функцій і рівнями цінності для бізнесу. Кібератака або зловмисник, який скомпрометував одну робочу станцію в зоні довіри, може переміститися вбік, щоб скомпрометувати набагато більш чутливі активи.

Модель безпеки з нульовою довірою розширює цей підхід, щоб покращити безпеку, а також зменшити складність. Модель доступу з нульовою довірою (ZTA) використовує ідентичність як периметр, а не автоматично передбачає довіру для будь-якої сутності, яка може отримати доступ до сегменту мережі. Модель нульової довіри встановлює стандарт, згідно з яким не можна припускати довіри до машин, додатків або користувачів, доки їхню особу не буде автентифіковано та доступ авторизовано відповідно до політики безпеки. Цей підхід використовує ідентифікаційні дані та облікові дані для створення безпечного середовища, і навіть при цьому надає авторизацію лише для обмеженого набору взаємодій і лише протягом необхідного періоду

Замість того, щоб переобладнувати системи такими підходами ізоляції, як брандмауери та VPN, сучасні розподілені, багатосторонні, масштабовані IT/OT операції потребують безпеки, яка базується на ідентифікації та забезпечує дотримання ZTA. Підхід ZTA застосовний не лише для людей і машин, але й для всіх людей, машин, додатків і даних, які складають операцію. Це означає, що операторам більше не потрібно погоджуватися на компроміси безпеки у своєму бізнесі, які є побічним продуктом застарілого дизайну, який неможливо адаптувати до сучасних мереж.

Xage спрощує керування доступом, надаючи єдину систему для керування та застосування політик безпеки доступу без довіри в усьому середовищі. Xage призначає ідентифікатор кожному користувачеві, машині, взаємодії та фрагменту даних, щоб уможливити застосування чітких політик доступу та примусового виконання.

Xage посилює рівень безпеки організації, надаючи сучасні можливості автентифікації та авторизації в застарілому середовищі (надійні паролі, MFA тощо). Xage створено як високонадійну та стійку мережу кібербезпеки, яку можна розгорнути як накладання поверх існуючих архітектур і систем без необхідності заміни обладнання чи змін мережі.

Крім того, оскільки весь доступ до системи контролюється та реєструється в захисті від несанкціонованого доступу Fabric, це забезпечує видимість усіх взаємодій ОТ (користувача, програми, машини).

Сучасна система має розгортання на місцях/заводах, у центрі керування, в центрі обробки даних і в хмарі, із взаємодією між людьми, машинами, програмами та даними через ці розгортання та зовнішні сторони. Сучасні підходи необхідно розширити, щоб, коли користувачеві або програмі потрібен доступ до ресурсу, його можна було надати, не відкриваючи «діри» для зловмисників. Застарілі інструменти, які використовуються сьогодні, просто не забезпечують такого рівня деталізації [9].

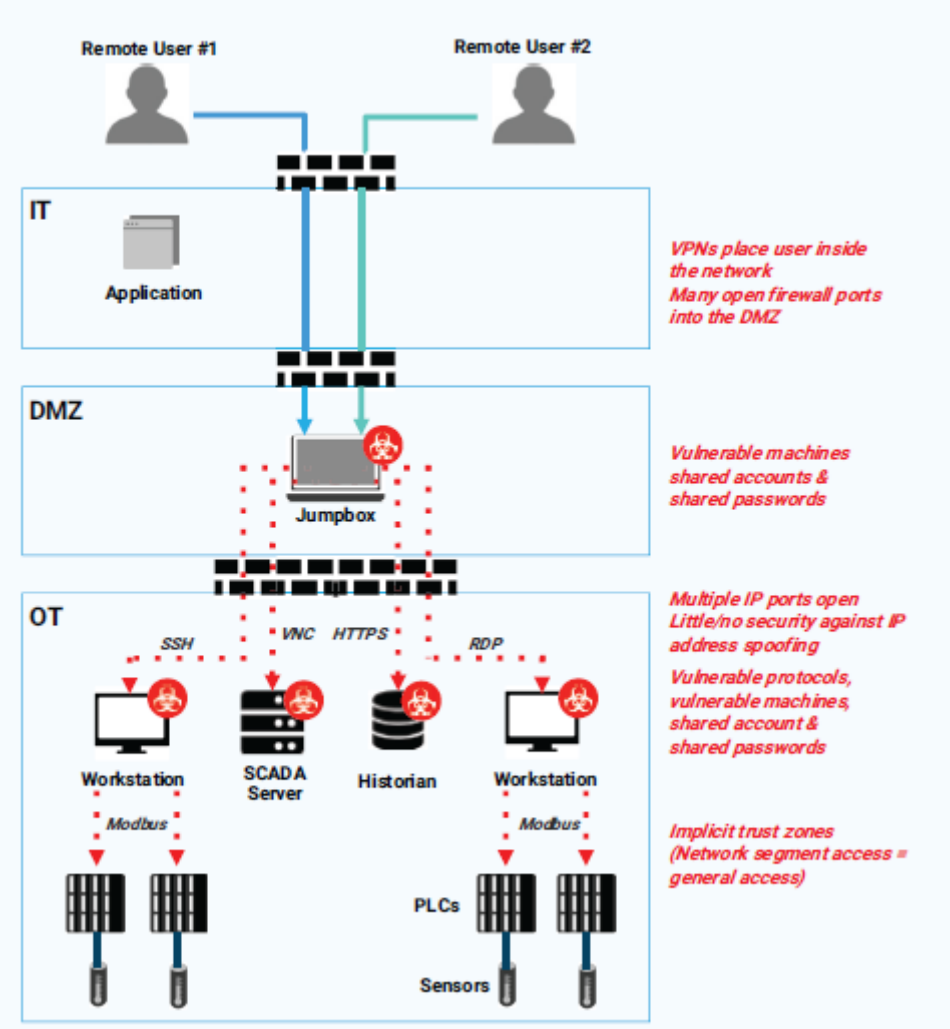

Рис.3.1. Вразливе середовище

Починаючи з межі середовища, Xage поширюється на IT підприємства, хмару та всі взаємодії між ними. Fabric створює цілісну безпеку від периферії до хмари з вбудованими складними можливостями вивчення політики та керування, що забезпечує дійсно безпечний віддалений доступ до середовища.

Віддалений доступ без довіри

Xage забезпечує безпечний віддалений доступ до середовищ OT і забезпечує точне керування доступом на основі ідентичності до польових і заводських активів. Xage спрощує керування доступом і замінює існуючі засоби контролю безпеки (наприклад, брандмауери, VPN, Jump Boxes), щоб полегшити безпечний віддалений доступ, усуваючи складність і знижуючи експлуатаційні витрати. У минулому віддалений доступ до активів OT надавався на основі сайту або зони. Якби технік міг отримати доступ до одного активу на сайті, він міг би отримати доступ до будь-чого, без ведення журналів або відповідальності за те, що вони робили. У Xage кожна подія

доступу має бути авторизована та автентифікована, а MFA доступна для окремих активів OT. Віддалений доступ Xage Zero Trust Remote Access дозволяє:

— Безпечний доступ через OT DMZ за допомогою проксі-сервера Xage та можливостей тунелювання з розривами протоколів для різних протоколів (наприклад, SSH, HTTP/S, RDP, VNC, Modbus тощо)

— Деталізована ідентифікація та віддалений доступ на основі ролей до певних активів (а не лише зон довіри) відповідно до політики безпеки, автоматично організованої наскрізно, без необхідності змінювати обліковий запис, актив або брандмауер

— Припинення протоколу, сеансу та шифрування на вузлі Xage, щоб прямий зв’язок із захищеними активами ніколи не дозволявся

— Вбудований контроль доступу (наприклад, блокування певних операцій на основі ідентичності) і моніторинг (наприклад, моніторинг через плече, запис сеансів і дій)

— Захищені від втручання журнали аудиту для всіх дій і взаємодій Забезпечує відповідність нормам і стандартам, таким як NERC-CIP і IEC 62443

— Нульовий доступ до додатків для настільних комп’ютерів, таких як FactoryTalk і RocLink, дозволяє технікам віддалено використовувати клієнт-серверні програми для OT через з’єднання, яке є набагато більш контрольованим і безпечним, ніж стандартна VPN.

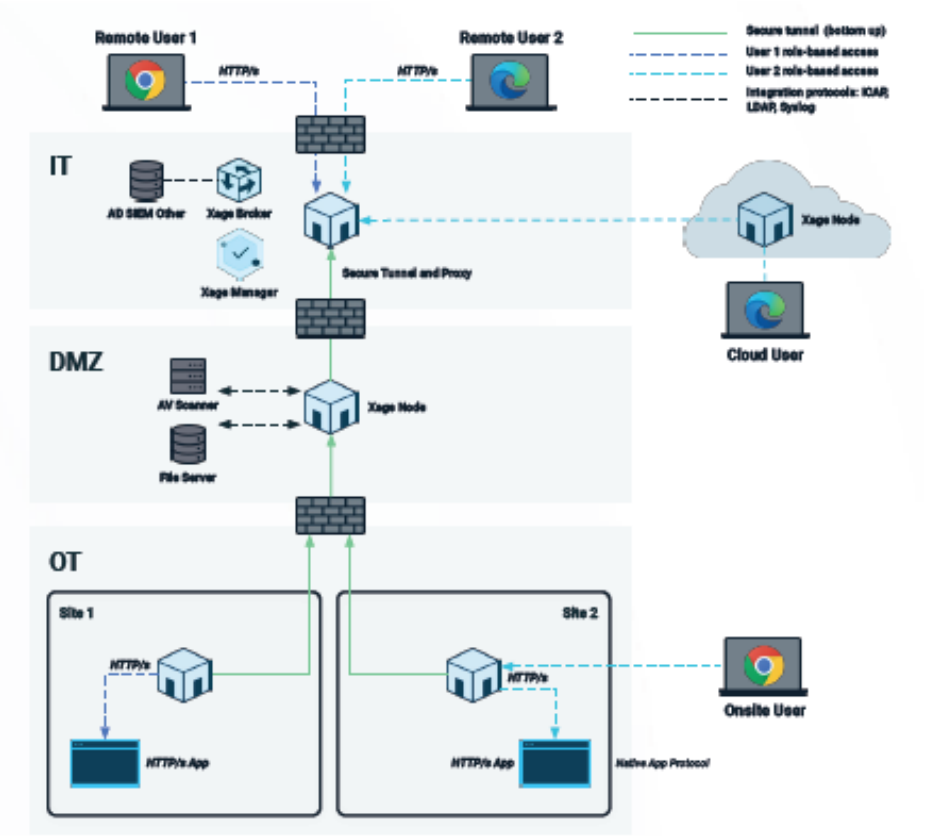

Рис.3.2. Інтеграція технології Zero Trust із існуючими системами організації

Віртуальний операційний центр Xage

Віртуальний операційний центр дозволяє технікам у різних місцях бачити той самий набір робочих екранів і додатків, забезпечуючи більш плавну співпрацю між місцевими та віддаленими техніками. Цей перегляд із кількома моніторами забезпечує численні операційні переваги без шкоди для засобів контролю безпеки, що є основними цінностями Xage:

Забезпечується можливість віддаленого відображення упорядкованого вигляду з кількох окремих дисплеїв на екранах будь-якої конфігурації з можливістю управління функціями читання та запису.

Організовується спільний доступ до кількох віддалених моніторів, які можуть бути об’єднані в одне вікно браузера або представлені в окремих вікнах для налаштування їх розташування на персональних дисплеях користувачів.

Надається обмежений або привілейований доступ для віддалених користувачів без створення вразливостей у захисті чутливих технологій оперативного управління (OT).

Xage Insights і Xena AI Copilot

Платформа Xage Fabric включає механізм аналізу під назвою Xage Insights і AI Copilot на базі новітніх технологій Generative AI під назвою Xena.

Xage Insights

Xage Insights забезпечує глибоку видимість доступу користувачів і пристроїв, а також дії у середовищі. Він може показати масу корисної інформації, яку можна негайно використати для покращення безпеки, наприклад:

- У скількох і в яких облікових записах MFA ще не ввімкнено. Застосування MFA є одним із найкращих способів запобігти кібератакам. Зловмисники не зламуються, вони входять.
- З якими пристроями не пов’язана політика доступу. Визначивши пристрої без політики доступу, можна визначити, де є прогалини у безпеці, і застосувати політики для їх захисту.

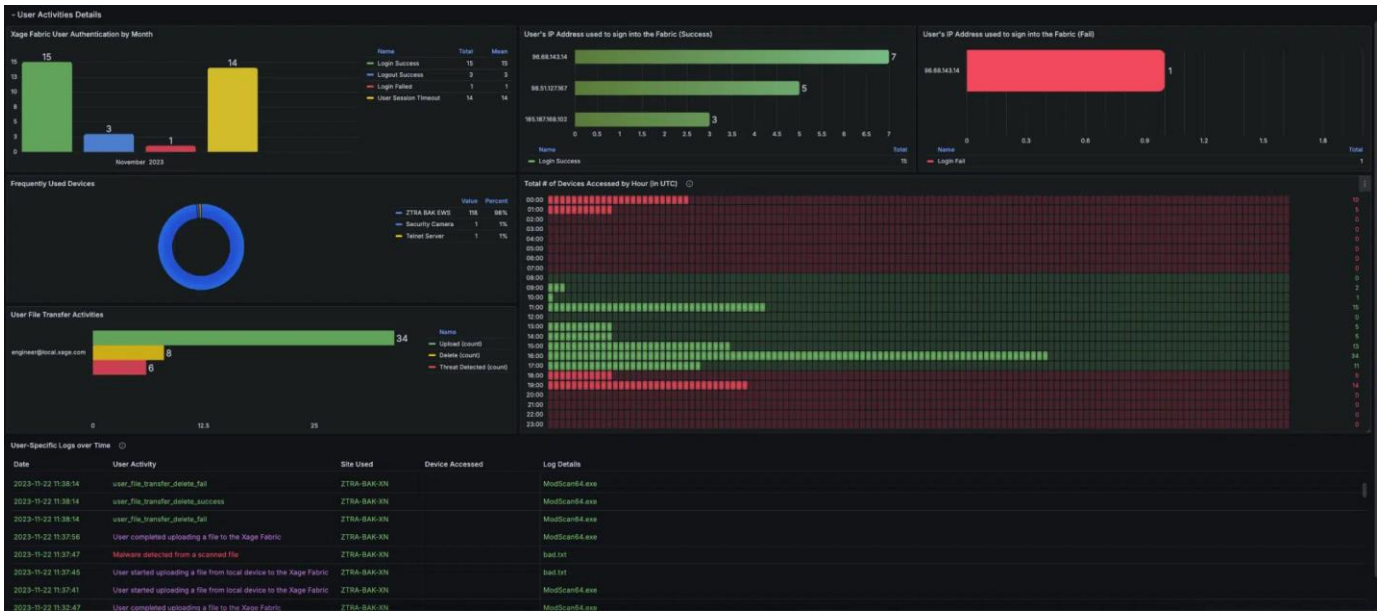

Рис.3.3. Xage Insights

Xage AI (Xena)

Xena дає адміністраторам і операторам простий спосіб ставити запитання щодо їхніх даних, використовуючи її можливості для покращеного інтелекту. Він надає корисну інформацію та пропозиції, які спеціально розроблено для середовища, включаючи глибокі аналізи активності у середовищі, нових загроз і керованих заходів щодо виправлення.

Використовуючи штучний інтелект, який забезпечує глибоке бачення шляхів доступу та поведінки користувачів від периметра до глибинного ядра середовища, Xena показує, де саме можуть бути ці критичні шляхи атаки. Тоді адміністратори безпеки та оператори можуть ефективно використовувати саму Xage Fabric для розгортання відповідних політик безпеки та примусового виконання саме там, де вони найбільше потрібні.

Система Xage забезпечує реалізацію політик доступу на основі принципу нульової довіри, підтримує багаторівневу багатофакторну автентифікацію (MFA) та швидке скасування прав доступу. Завдяки інтеграції з модулем Xena, система надає можливість оперативного визначення, де саме ці функції найбільш потрібні в існуючому середовищі.

Приклади запитів, які можуть бути адресовані Xena, включають:

Визначення геолокацій, з яких користувач здійснив доступ до пристрою або увійшов у систему.

Ідентифікація підозрілої активності в системах.

Виявлення політик, які потребують вдосконалення.

Генерація звіту про стан безпеки, призначеного для обміну з керівництвом.

Надання коду для виконання завдань, таких як увімкнення MFA для користувача, призупинення облікового запису користувача або зміна пароля в Active Directory.

Зазначений функціонал спрямований на підвищення рівня безпеки та зручності управління доступом у корпоративному середовищі.

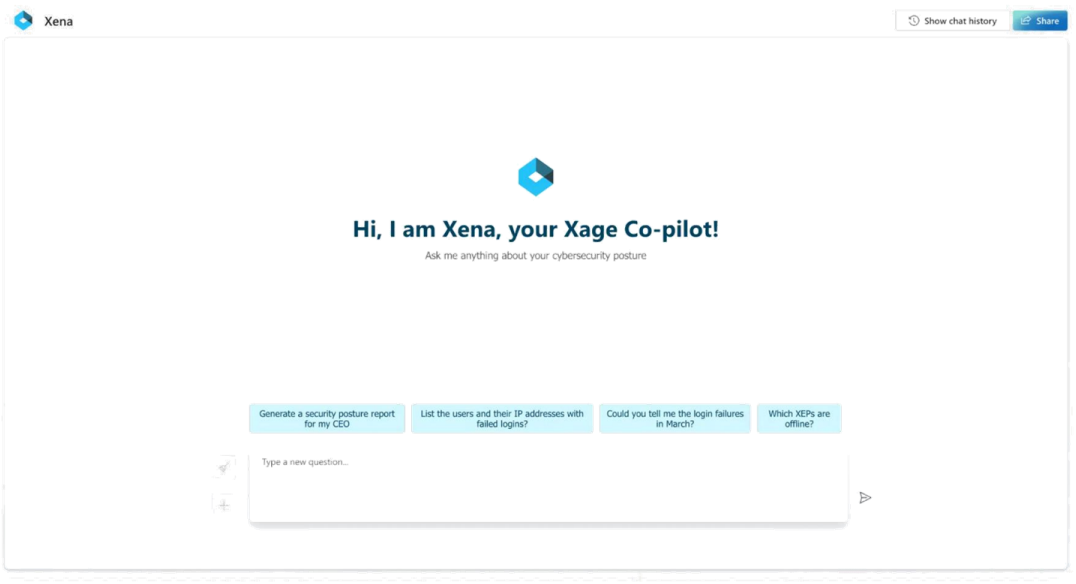

Рис.3.4. Модуль Xena

Платформа Xage Fabric

Платформа Xage Fabric — це стійка розподілена мережа кібербезпеки з високою доступністю, яка лежить в основі всіх продуктів і послуг Xage. Унікальна архітектура платформи Xage Fabric дозволяє Xage надавати продукти нового покоління з багатьма перевагами перед іншими рішеннями Zero Trust Network Access (ZTNA) і Privileged Access Management.

Платформа Xage Fabric побудована на основі технології розподіленої книги, яка автоматично розподіляє критичну інформацію між вузлами в структурі та використовує криптографічні консенсусні процеси під назвою Shamir's Secret Sharing і Federated Byzantine Agreement для запобігання неавторизованому доступу до цих даних. Серед основних переваг цього підходу:

1. Xage Fabric продовжує застосовувати політики нульового довірчого доступу навіть при відключенні від широкого Інтернету або навіть WAN компанії. На відміну від інших рішень ZTNA, Xage не потребує безперервного з’єднання з хмарою для проведення автентифікації та авторизації, а також для застосування політик доступу та дозволу чи обмеження доступу локально відповідно до політики. Xage

залишається повністю працездатним у віддалених середовищах із забороненим, погіршеним, переривчастим або прихованим (DDIL) підключенням.

2. Xage Fabric зберігає облікові дані та політики локально на кожному сайті та навіть на кожному рівні середовища, не вимагаючи дублювання вручну.

3. Xage Fabric використовує розподілене сховище облікових даних, розподіляючи облікові дані між кількома вузлами Fabric, щоб кібератаки не змогли викрасти сховище облікових даних. Облікові дані є популярною мішенню для крадіжок, їх часто викрадають і продають у темній мережі для подальших атак. Xage запобігає цьому [10].

Xage контролює взаємодію між кількома ідентифікаторами, кількома сайтами та кількома сторонами за допомогою системи єдиного входу (SSO) і багатофакторної автентифікації (MFA). Security Fabric від Xage починається зі створення ідентичності для машин, користувачів, програм і даних. Крім того, він створює універсальний рівень керування доступом на основі ідентичності, який забезпечує безпечний, детальний контроль над різними взаємодіями в IT/OT середовищі. Точне управління включає відображення потоків і керування на основі параметрів відповідно до політик і ролей ідентифікаторів, залучених у взаємодію.

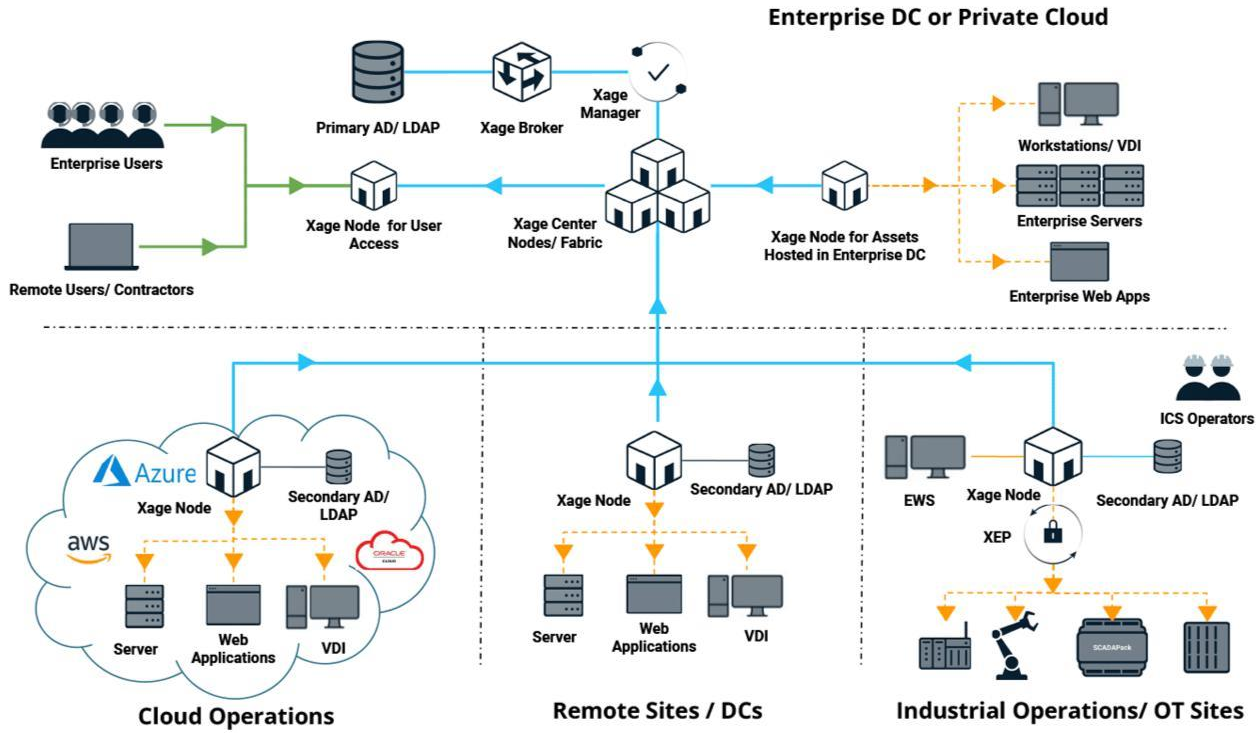

Рис.3.5. Розгортання платформи Xage Fabric в організації

На рис.3.5. зображено архітектуру управління доступом і безпеки в розподілених IT- та OT-системах із використанням рішень Xage. Архітектура включає наступні ключові компоненти та потоки:

Верхня частина (Enterprise DC або приватна хмара):

Enterprise Users (користувачі компанії): підключаються через LDAP/Active Directory (AD) до Xage Node для доступу до системи.

Xage Manager: централізована панель управління для керування користувачами, політиками безпеки та доступом.

Xage Broker: взаємодіє з первинним AD/LDAP для автентифікації та передачі політик безпеки.

Xage Center Nodes/Fabric: забезпечує безпечний доступ і розподілення інформації між різними компонентами.

Сервери, робочі станції, програми: працюють в межах приватного центру даних (Enterprise DC) із захищеним доступом через Xage Node.

Середня частина:

Cloud Operations (Хмарні операції):

Інтеграція з платформами Azure, AWS та Oracle Cloud.

Xage Node забезпечує доступ до хмарних сервісів, веб-додатків і віртуальних середовищ (VDI).

Секундарний AD/LDAP синхронізується з первинним для підтримки політик безпеки.

Remote Sites / DCs (Віддалені об’єкти / ЦОДи):

Віддалені сервери, веб-додатки та віртуальні середовища (VDI) взаємодіють із Xage Node.

Секундарний AD/LDAP дозволяє керувати доступом і автентифікацією локально.

Нижня частина (Industrial Operations/OT Sites):

ICS Operators (Оператори індустріальних систем): отримують доступ до систем через Xage Node.

EWS (Engineering Workstations): взаємодіють із системами управління через XEP (Xage Enforcement Point).

SCADA/PLC: контрольні системи автоматизації та логічні контролери, інтегровані в OT-середовище.

Xage Node: забезпечує безпеку та контроль доступу для OT-обладнання та інженерних систем.

Основні функції:

Захищений доступ користувачів і пристроїв через багаторівневу автентифікацію.

Інтеграція з існуючими AD/LDAP для централізованого управління.

Гібридне середовище: підтримка локальних, хмарних і віддалених інфраструктур.

Ця архітектура підходить для компаній, які використовують як традиційні IT-системи, так і операційні (OT) системи, забезпечуючи єдиний підхід до безпеки та управління доступом.

Платформа Xage Fabric надає низку переваг, спрямованих на забезпечення високого рівня безпеки та ефективності управління доступом в інформаційних системах. До основних переваг належать:

Реалізація нульового довірчого контролю для окремих взаємодій між користувачами, програмами, комп'ютерами, пристроями та даними. Контроль здійснюється у напрямках північ-південь і схід-захід, як у межах зон довіри, так і поза ними, через периферійні вузли, центри керування, центри обробки даних і хмарні середовища.

Запобігання порушенням безпеки за допомогою контролю бокового переміщення, автоматичної ротації облікових даних та застосування багатофакторної автентифікації для кожного активу.

Використання динамічної рольової політики взаємодії, що замінює статичні правила брандмауера, для спрощення управління доступом.

Забезпечення віддаленого та локального доступу для користувачів, програм, машин і даних із підтримкою багатокористувацької співпраці.

Впровадження багатофакторної автентифікації як накладання, що не потребує змін у конфігурації активів.

Реалізація універсального управління ідентифікацією (IAM) із підтримкою застарілих і сучасних пристроїв і програм, включаючи систему єдиного входу (SSO) та інтеграцію з кількома постачальниками.

Можливість управління розгортанням у середовищах з кількома постачальниками ідентифікації та інтеграцією з Active Directory.

Використання багатофакторної автентифікації на кожному рівні доступу, включно з пристроями та міжмережевими переходами.

Обмін даними на основі принципу нульової довіри (ZTDE) із забезпеченням автентичності, цілісності, конфіденційності та контролю в середовищах OT/IT/Cloud/Ecosystem.

Захищене від втручання розподілене сховище для зберігання журналів аудиту, записів взаємодії та операційних даних.

Розподілене сховище паролів із автоматичною ротацією облікових даних для запобігання атакам, що використовують викрадені облікові записи або їх експлуатацію під час початкового доступу чи бокового переміщення.

Ці можливості дозволяють платформі Xage Fabric забезпечувати комплексний підхід до управління доступом і безпеки у складних інформаційних екосистемах [13].

3.2. Технологія забезпечення безпеки організації на базі рішення Xage Zero Trust

Нульовий довірчий доступ для програм, специфічних для інформаційної системи

Система Xage забезпечує функціонал Zero Trust Remote Access, призначений для безпечного віддаленого доступу до клієнт-серверних програм, специфічних для технологій оперативного управління (OT), таких як FactoryTalk, Studio5000 тощо. Це дозволяє вирішувати критичну проблему безпечного підключення сторонніх пристроїв або постачальників до корпоративного середовища, уникаючи ризиків, пов’язаних із можливим впровадженням шкідливого програмного забезпечення чи незареєстрованою активністю.

Zero Trust Remote Access реалізує значно вищий рівень безпеки, ніж традиційні VPN-рішення.

Принцип роботи:

Аутентифікація користувача

Користувач здійснює вхід у Xage Fabric, після чого встановлюється пряме з’єднання між ноутбуком користувача (або стороннім пристроєм) і точкою утримання нульової довіри у Fabric. Така точка може знаходитися у хмарі, IT-середовищі, iDMZ або OT.

Авторизація та створення тунелів нульової довіри

Після перевірки авторизації для доступу до цільової периферійної системи, Fabric створює тунелі нульової довіри. Ці тунелі обмежують доступ до окремих активів і протоколів відповідно до встановлених політик. Захист тунелів забезпечується цифровими підписами в Fabric і багаторівневою багатофакторною автентифікацією (MFA).

Безпосередня робота з цільовою системою

Користувач отримує доступ до цільової системи через клієнт-серверні програми безпосередньо зі свого пристрою. При цьому Xage Fabric ізолює ноутбук від інших сегментів OT, IT та хмарної мережі, забезпечуючи безпеку всього середовища.

Ключові переваги:

Виключення необхідності довіряти некерованим пристроям, що підключаються до мережі.

Захищені тунелі нульової довіри з чітко визначеними політиками доступу.

Підтримка ізоляції пристроїв від критичних елементів мережі.

Підвищення безпеки клієнт-серверних з’єднань у середовищах OT та IT.

Цей підхід дозволяє організаціям мінімізувати ризики і забезпечити безпеку навіть за умови використання сторонніх пристроїв.

Керування привілейованим доступом і керування доступом постачальника

Окрім віддаленого доступу, Xage пропонує привілейоване керування доступом як для внутрішніх користувачів, так і для сторонніх користувачів, а також до активів ICS, таких як системи SCADA, ПЛК і RTU.

Xage можна легко використовувати для надання співробітникам, постачальникам, постачальникам послуг та іншим партнерам контрольованого привілейованого доступу до активів, необхідних їм для виконання своїх зобов'язань у партнерстві. Xage дозволяє:

- Швидке надання облікових записів для внутрішніх і зовнішніх користувачів.
- Швидке налаштування політики найменших привілеїв для будь-якого користувача та активу
- Автоматична деактивація облікових даних і зміна паролів, щоб уникнути витоку або застарілих облікових записів від використання проти вас.
- Часовий доступ для обмеження доступу третіх сторін до мінімально необхідного періоду часу для виконання своїх завдань
- Відстеження та запис сеансів, щоб адміністратори могли відстежувати, що відбувається, і перевіряти минулі сеанси
- Виявлення облікового запису в активах
- Фільтрування команд на основі рівня привілеїв
- API для отримання облікових даних
- Ротація облікових даних, як автоматизована, так і вручну
- Підтримка широкого спектру систем і програм, включаючи сервери, робочі станції, хмарні робочі навантаження, мережеві елементи, бази даних, настільні програми типу клієнт-сервер тощо.
- Детальне журналювання аудиту з простою інтеграцією SIEM/SOAR

Єдиний вхід із кількома постачальниками ідентифікаційної інформації (IdP)

Xage забезпечує можливості єдиного входу (SSO) для операцій і активів підприємства. Це включає SSO для машин і додатків, які використовують промислові протоколи, і тих, які розгорнуті у віддалених місцях. Система єдиного входу на основі ідентичності гарантує, що взаємодія користувача, програми та комп'ютера захищена

та безперебійно контролюється незалежно від основної сегментації мережі. Xage SSO значно спрощує безпечний доступ до операційних активів через портал SSO, усуваючи потребу відновлювати IP-адреси, порти, програми та облікові дані для конкретних активів.

Крім того, Xage підтримує багатостороннє об'єднання служб ідентифікації внутрішніх і зовнішніх організацій, включаючи, наприклад, можливість об'єднання компаній-партнерів, які працюють над спільним проектом, щоб співробітники кожного партнера могли використовувати власні керовані облікові дані для доступу активи спільної інфраструктури.

Забезпечується можливість управління декількома постачальниками ідентифікаційної інформації (Identity Providers, IdP) для організації ефективного та безпечного процесу автентифікації. Це дозволяє інтегрувати різні системи управління ідентифікацією в рамках однієї платформи.

Оператори критичної інфраструктури можуть використовувати Xage для створення окремих ідентифікаторів (наприклад, облікових даних для входу) на кожному рівні та сайті з різними адміністраторами, щоб гарантувати, що компрометація корпоративних облікових даних IT не призведе до компромісу в OT. Це також гарантує, що компрометація одного сайту не призведе до компрометації всіх сайтів (або навіть інших активів на тому самому сайті). Крім того, операційні групи можуть зменшити складність процесу керування доступом для свого персоналу та покращити взаємодію з користувачами, а також блокувати атаки, використовуючи наступні унікальні можливості:

Мультивендорна підтримка IdP та інтеграція різних протоколів автентифікації

Забезпечується можливість управління кількома постачальниками ідентифікаційної інформації (Identity Providers, IdP) та доменами Active Directory (AD), що належать до різних зон безпеки або мережевих рівнів. Для цього підтримуються різні протоколи автентифікації, зокрема LDAP, SAML і ADFS, які можуть бути налаштовані для кожного IdP залежно від вимог безпеки.

Обмеження видимості активів до моменту автентифікації

Видимість активів і систем обмежується до успішного проходження автентифікації. Локальні та віддалені користувачі можуть отримати доступ до

ресурсів лише після автентифікації на рівні відповідного домену AD та виконання багатофакторної автентифікації (MFA), яка застосовується до рівня конкретного сайту чи зони.

Локальна автентифікація за умови втрати мережевого з'єднання

Забезпечується можливість для локальних користувачів здійснювати автентифікацію через AD рівня локального сайту навіть у випадках втрати підключення до мережі. Це підвищує стійкість до перебоїв у роботі мережевих систем.

Багаторівнева MFA із підтримкою різних методів і технологій

Реалізовано використання безпарольної, апаратної або біометричної багатофакторної автентифікації, яка може застосовуватися на кількох рівнях доступу. Система дозволяє зіставляти методи MFA із різними постачальниками ідентифікаційної інформації, забезпечуючи адаптивний підхід до безпеки.

Багатофакторна автентифікація (MFA)

Xage усуває проблеми з інтеграцією MFA в існуючі середовища. Забезпечуючи інтеграцію MFA з будь-яким пристроєм і програмою, Xage дозволяє організаціям додавати MFA до всіх своїх активів, спрощуючи керування та роботу захисту MFA на основі ідентифікації. Створені спеціально для підтримки випадків використання OT/IoT, високонадійна автентифікація та примусове забезпечення Xage надаються на межі та продовжують працювати, навіть якщо зв’язок із центром втрачено. Xage забезпечує багатофакторний доступ на основі ідентичності та з низькою затримкою навіть через переривчасті мережі та до віддалених ресурсів.

Можливості уніфікованої багатофакторної автентифікації (MFA) для розгорнутих активів (ICS та IoT, застарілих і нових):

- Дозволяє комплексний контроль доступу на основі ідентифікації пристрою та програми
- Xage Enforcement Point (XEP) забезпечує застосування MFA до будь-якої застарілої однофакторної або нульової системи, включаючи системи SCADA, ПЛК і RTU.

- Забезпечує стандартизацію методів багатофакторної автентифікації та поширює їх на базу розгортання програм, робочих станцій, пристроїв керування тощо.
- Забезпечує гнучкість у виборі та перемиканні між методами MFA (контакти, ключі, смарт-картки, програми автентифікації тощо)
- Забезпечує відповідність численним стандартам у різних сферах без необхідності заміни існуючих активів
- Забезпечує надійний аудит для всіх взаємодій між машинами та користувачами

Внутрішня сегментація з міжмашинним контролем доступу

Традиційні підходи до сегментації мережі використовують VLAN, внутрішні брандмауери та ACL. Ці підходи дорогі, складні в розгортанні та управлінні, і все ще не можуть забезпечити захист на рівні кожного пристрою. З Xage Zero Trust Segmentation і Microsegmentation можлива детальна сегментація, яка може обмежити доступ і зв'язок для кожного користувача та кожного пристрою. Це має вирішальне значення для запобігання бічним рухам і методам життя поза межами землі.

Розширюючи контроль доступу користувачів і додатків, Xage використовує підхід на основі ідентичності для контролю взаємодії між машинами всередині та між зонами довіри. Посвідчення для машин створюються з використанням комбінації мережевих, системних і прикладних характеристик машин і включають комбінацію IP, MAC, протоколу та версії програмного забезпечення/прошивки/апаратного забезпечення та таблиць пошуку даних.

Після створення ідентифікацій можна легко визначити політики для окремих машин або груп машин. Політики включають інформацію про місцезнаходження, час взаємодії, а також параметри, якими дозволено обмінюватися на основі окремих ролей машини. Крім того, Xage додатково забезпечує наскрізне шифрування на основі взаємодії та потоку, тобто лише вибрані взаємодії будуть зашифровані.

Межмашинний контроль доступу Xage дозволяє:

- Детальний і динамічний контроль взаємодії машин (без статичних правил)

- Ідентифікатори для всіх машин із можливістю виявлення змін і шахрайських машин
- Наскрізне шифрування для взаємодії за допомогою автоматичного тунелювання IPSec (тунелі автоматично налаштовуються та керуються на основі політики для всіх взаємодій)
- Ідентифікація та захист спуфінгу повідомлень
- Немає впливу на автоматизацію та контроль (накладні витрати на рівень затримки мікросекунд)
- Можливості внутрішньої сегментації та брандмауера без необхідності реструктуризації підмережі середовища
- Забезпечує керування сегментацією для дотримання принципів зон і каналів IEC 62443 без ускладнень впровадження та адміністрування [11].

Xage Enforcement Point усуває потребу у внутрішніх брандмауерах для сегментації

Xage пропонує точку застосування політики, яка за замовчуванням забороняє доступ до всього, що стоїть за нею, а також служить шлюзом автентифікації, фільтром пакетів і внутрішнім брандмауером сегментації. Xage Enforcement Point (XEP) надає кращі можливості внутрішньої сегментації, ніж брандмауери, з меншою вартістю та навантаженням на керування. XEP дозволяє локально керувати обліковими записами та застосовувати політику, а також діє як прозорий проксі-сервер безпеки. Це може дозволити програмно визначене двонаправлене керування трафіком замість функціональності діода даних. XEP доступний як як апаратне забезпечення, так і у віртуалізованому вигляді.

Обмін даними Xage Zero Trust (ZTDE)

Обмін даними Zero Trust від Xage дозволяє організаціям співпрацювати між усіма платформами даних, одночасно забезпечуючи автентичність, цілісність і конфіденційність між різними програмами, машинами, організаціями та місцями, дозволяючи багатьом учасникам безпечно отримувати доступ до даних у будь-якому місці. Операційне рішення Xage для захисту даних захищає від несанкціонованого втручання та плавно копіює дані та ідентифікаційну інформацію даних (тобто

відбиток безпеки даних або метадані) через Xage Fabric у будь-якому місці, де дані споживаються.

У рамках цього процесу Xage Fabric забезпечує надійну, динамічну та безпечну передачу даних «точка-точка» через розподілену структуру, долаючи проблеми переривчастого підключення та складної мережевої архітектури. Тепер організації можуть безпечно обмінюватися даними від периферії до центру обробки даних і до хмари, а також від хмари/центру обробки даних до периферії, створюючи нові операційні ідеї та інновації, а також забезпечуючи клієнтам і постачальникам додатки на основі даних.

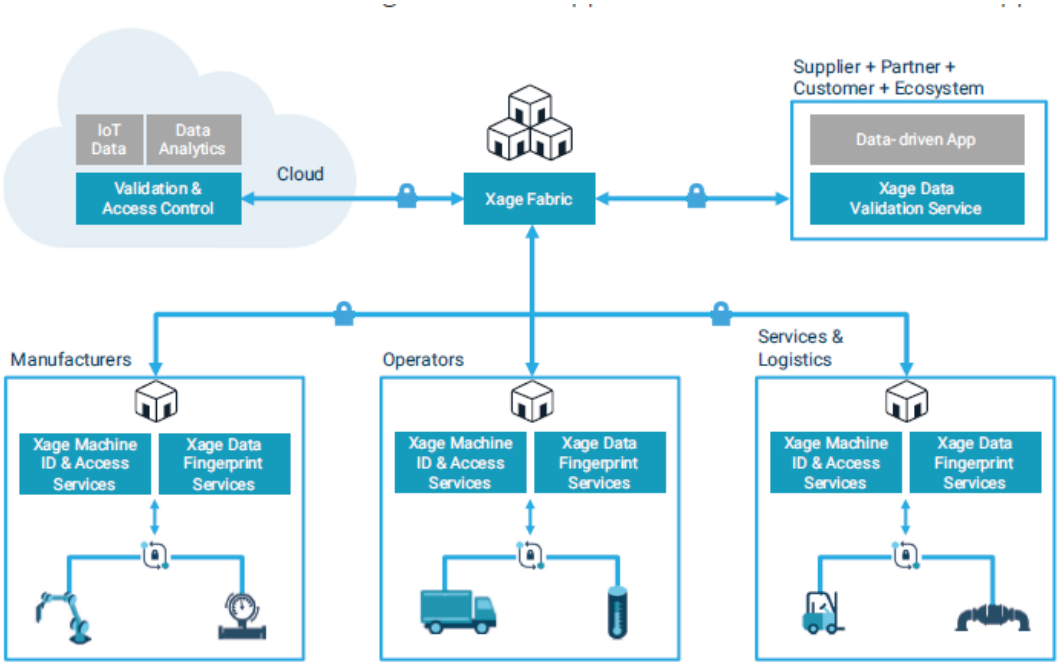

Рис.3.6. Zero Trust Data Exchange (ZTDE)

Пропозиція Zero Trust Data Exchange (ZTDE) забезпечує динамічний і контрольований обмін даними із захищеною від несправностей автентичністю, цілісністю та конфіденційністю:

- **Автентичність:** Коли дані створюються, вони підписуються цифровим підписом за допомогою унікального ключа, який передається через довірену незмінну книгу Fabric, що гарантує походження даних. Відбитки пальців пристроїв, що зберігаються в Xage Fabric, забезпечують надійний запис усіх пристроїв, який можна

зіставити з метаданими даних, щоб ідентифікувати пристрій, з якого надходять дані, і гарантувати автентичність джерела даних.

- **Цілісність:** Коли дані обмінюються та вилучаються, Xage забезпечує цілісність за допомогою відбитків даних (криптографічних хешів), які реплікуються в Fabric, що дозволяє перевіряти цілісність даних у будь-якому місці за потреби.
- **Конфіденційність і контроль доступу:** Fabric також дозволяє організаціям встановлювати керування ідентифікацією та детальний контроль доступу за пристроєм, програмою, користувачем і потоком даних, щоб захистити дані з неперевершеною точністю – наприклад, за темою чи часом – аж до рівня окремих значень даних, якщо потрібно.

Завдяки механізму реплікації Xage Fabric, що захищений від несанкціонованого доступу, організації можуть безпечно та спільно обмінюватися даними наскрізно через всю платформу даних. Точки Xage Fabric і Xage Enforcement Points (XEP) динамічно й автоматично встановлюють зашифрований тунель для зв'язку щоразу, коли вони виявляють дві системи, які намагаються зв'язатися через мережу.

Крім того, вузли Fabric виконують функцію безпечної передачі даних, коли дані та пов'язану з ними інформацію безпеки потрібно перемістити з одного місця в інше, але прямий тунель «точка-точка» не може бути встановлений через архітектуру мережі та/або переривчасте підключення до мережі. . Ці методи передачі захищають дані під час їхнього переміщення по мережі, звільняючи дані від традиційних OT-розділів, а також зберігаючи безпеку та відповідність стандартним моделям багаторівневої безпеки [9].

Підтримка Xage для MITER ATT&CK Framework for Industrial Control Systems

Платформа MITER ATT&CK для ICS стала галузевим стандартом для розуміння тактики, прийомів і процедур (TTP), які використовуються кібератаками під час спостережуваних атак у реальному світі. Платформа Xage Fabric пропонує або повне запобігання, або часткове пом'якшення понад 90% TTP, перелічених у Framework [12].

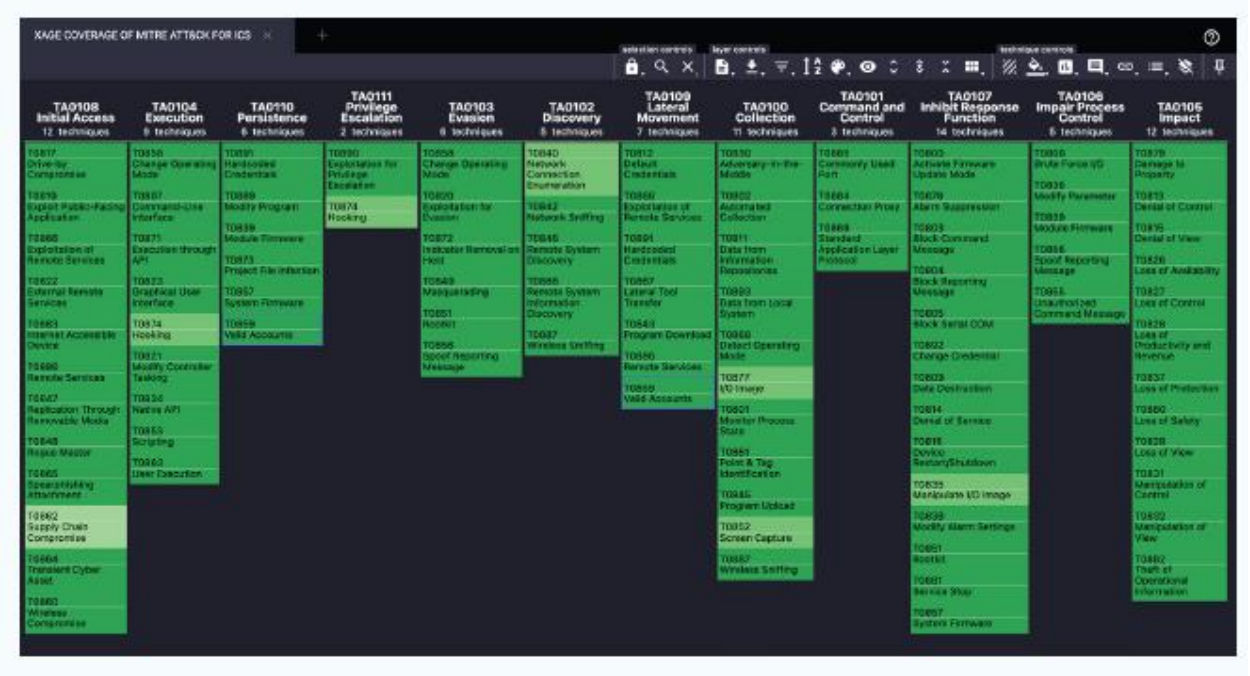

Рис.3.7. Підтримка MITER ATT&CK

Технічні партнери та інтеграція Xage

Xage пропонує інтеграцію з кількома партнерськими технологіями для забезпечення повного охоплення безпеки, запобігання атакам, виявлення та реагування.

Збагачення запасів активів

Xage може отримувати інформацію про інвентаризацію активів від постачальників засобів виявлення активів і збагачувати цей інвентар більш детальною інформацією та видимістю доступу користувачів і поведінки щодо активів, а також створювати та застосовувати політику, MFA тощо щодо всіх виявлених активів.

Виявлення аномалій і реагування на загрози

Xage інтегрується з партнерами з виявлення аномалій, щоб забезпечити глибоку видимість і журнали аудиту з кожного рівня моделі Перд'ю, забезпечуючи багатий набір даних, який можуть використовувати рішення для виявлення аномалій для виявлення непомітної поведінки атак і методів живих позаземних (LOTL) глибоко всередині OT середовище. Xage також дозволяє негайно реагувати, наприклад обмежити права доступу облікових записів, які демонструють аномальну або зловмисну поведінку.

Адаптивне керування доступом через інтеграцію з виявленням кінцевої точки та відповіддю/розширеним виявленням та відповіддю (EDR/XDR)

Xage інтегрується з постачальниками EDR/XDR, щоб забезпечити адаптивний контроль доступу у відповідь на спостережувану ризиковану поведінку або сигнали розвідки про загрози. Наприклад, якщо XDR спостерігає, що певна кінцева точка виконує ризиковану поведінку або зв'язується з відомою зловмисною IP-адресою, Xage може автоматично налаштувати політику доступу цієї кінцевої точки, щоб обмежити можливість потенційного зловмисника рухатися вбік від скомпрометованої кінцевої точки. Це забезпечує точне, цілеспрямоване коригування політики доступу на основі спостережуваного рівня ризику, а не підхід «все або нічого», який полягає в тому, щоб просто повністю припинити доступ пристрою до мережі.

Збагачення журналів для OT Access за допомогою інтеграції SIEM/SOAR

Xage фіксує докладні журнали аудиту подій і активності користувачів і може надсилати їх до будь-якої системи SIEM/SOAR для виявлення безпеки, дослідження та реагування з боку групи безпеки або постачальника керованих послуг безпеки (MSSP) [10].

3.3. Розроблення рекомендацій щодо захисту систем організації на базі технології Zero Trust

На основі аналізу моделі Zero Trust, а також інноваційних рішень та практик у галузі забезпечення кібербезпеки, запропоновано такі рекомендації для підвищення ефективності безпеки інформаційних систем організації:

1. Впровадження принципу нульової довіри (Zero Trust)

Забезпечити контроль доступу до ресурсів організації на основі принципу мінімальних привілеїв (Least Privilege Access), зводячи до мінімуму обсяг доступу навіть для привілейованих користувачів.

Використовувати багатофакторну автентифікацію (MFA) на кожному рівні доступу до активів, включаючи локальних і віддалених користувачів.

Реалізувати динамічні політики доступу, які враховують не лише ідентифікаційні дані, але й поведінкові характеристики користувачів та пристроїв.

2. Інтеграція з різними постачальниками ідентифікаційної інформації (IdP)

Налаштувати роботу з кількома IdP, підтримуючи різні протоколи автентифікації, зокрема LDAP, SAML і ADFS.

Забезпечити сумісність нових систем з існуючими активами та інфраструктурою організації, підтримуючи універсальне управління доступом (IAM).

3. Захист критичних інфраструктур

Використовувати захищений віддалений доступ, який виключає традиційні VPN і дозволяє обмежувати видимість активів до моменту автентифікації.

Реалізувати Zero Trust Remote Access для клієнт-серверних програм, специфічних для операційних технологій (OT), з метою виключення неконтрольованого доступу сторонніх пристроїв.

Забезпечити захист від бокового руху в мережі шляхом автоматизованої ротації облікових даних та застосування контролю на кожному стрибку.

4. Автоматизація та адаптивність політик безпеки

Використовувати технології аналітики поведінки та машинного навчання для виявлення аномальної активності та автоматичного реагування на загрози.

Розгорнути рішення для автоматичного моніторингу відповідності пристроїв корпоративним політикам безпеки та контролю стану їх захисту.

5. Підвищення стійкості до збоїв у мережі

Налаштувати можливість локальної автентифікації користувачів через AD, навіть у разі втрати підключення до основної мережі.

Використовувати розподілені сховища даних для журналів аудиту, записів взаємодії та облікових даних, захищені від втручання зловмисників.

6. Освітні заходи та підготовка персоналу

Проводити регулярні тренінги для співробітників з використання нових технологій безпеки, особливо в частині роботи з багатофакторною автентифікацією та системами управління ідентифікацією.

Включати сценарії симуляцій атак для підвищення готовності команди реагування на інциденти.

Застосування цих рекомендацій дозволить організації не лише відповідати сучасним вимогам до кібербезпеки, а й забезпечити довгострокову стійкість до нових загроз.

ВИСНОВКИ

У роботі проведено дослідження проблеми забезпечення безпеки інформаційних систем організації на базі Zero Trust. Визначено основні загрози кібербезпеці, а також обґрунтовано важливість застосування моделей безпеки, що ґрунтуються на принципі нульової довіри для забезпечення надійного захисту.

Проаналізовано існуючі підходи до забезпечення безпеки інформаційних систем за допомогою технологій Zero Trust. Виявлено ключові елементи таких рішень, зокрема багатофакторну автентифікацію, контроль доступу на основі політик, а також використання розподілених систем для контролю доступу та моніторингу користувачів.

Досліджено методи та засоби впровадження технології Zero Trust для захисту організаційних інформаційних ресурсів. Розглянуто можливості застосування різних рішень, таких як Xage, які дозволяють інтегрувати захист на рівні доступу та комунікацій для всіх типів користувачів і пристроїв.

Проаналізовано порядок впровадження технологій на базі Zero Trust у корпоративне середовище, зокрема забезпечення безпечного доступу до корпоративних систем та даних з урахуванням вимог до конфіденційності, цілісності та доступності інформації.

Зважаючи на постійно зростаючі кіберзагрози, важливо постійно вдосконалювати та адаптувати стратегії безпеки інформаційних систем на основі принципу нульової довіри. Реалізація технологій Zero Trust повинна передбачати не лише контроль доступу до корпоративних систем, а й інтеграцію з іншими елементами інфраструктури, такими як моніторинг аномальної поведінки користувачів, управління ризиками та автоматичне реагування на загрози.

Розроблено рекомендації для організацій щодо ефективного застосування технології Zero Trust, зокрема, створення гнучкої системи автентифікації, налаштування політик безпеки та моніторингу доступу для мінімізації ризиків від атак та витоків інформації.

Запропоновано ключові стратегії для інтеграції Zero Trust у корпоративні IT-системи, що дозволяє забезпечити безпечну роботу гібридних працівників, знижуючи можливі загрози та вразливості, пов'язані з доступом до корпоративних ресурсів з різних точок мережі.

Таким чином, впровадження технології Zero Trust є необхідною умовою для забезпечення високого рівня безпеки інформаційних систем організації та захисту її цифрових активів від зростаючих кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Kumar, I. (2023). Emerging Threats in Cybersecurity: A Review Article. International Journal of Applied and Natural Sciences, 1(1), 01–08. Retrieved from https://bluemarkpublishers.com/index.php/IJANS/article/view/2

2. New Technologies in Cybersecurity | Combatting the Latest Threats. Explore Cybersecurity Degrees and Careers | CyberDegrees.org. URL: https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/ (дата звернення: 23.10.2024).

3. Exploring Access Control Models: Building Secure Systems in Cybersecurity. Tripwire | Security and Integrity Management Solutions. URL: https://www.tripwire.com/state-of-security/exploring-access-control-models-building-secure-systems-cybersecurity (дата звернення: 30.10.2024).

4. Zero Trust Architecture: The Key to Modern Cybersecurity. *Trio Blog*. URL: https://www.trio.so/blog/zero-trust-architecture/ (дата звернення: 02.11.2024).

5. NIST Special Publication 800-207, Zero Trust Architecture, COMPUTER SECURITY, August 2020 URL: https://doi.org/10.6028/NIST.SP.800-207

6. Top 5 Best Practices for Implementing Zero Trust Security - DataGroupIT. DataGroupIT. URL: https://datagroupit.com/top-5-best-practices-for-implementing-zero-trust-security/ (дата звернення: 06.11.2024).

7. Xage Zero Trust Access. Xage Security. 2024 URL: https://info.xage.com/hubfs/Datasheets/Xage%20Zero%20Trust%20Access.pdf (дата звернення: 06.11.2024).

8. Xage Security and Darktrace Partner to Enhance Zero Trust Protection for Commercial Critical Infrastructure Environments. Darktrace | Cyber security that learns you. URL: https://darktrace.com/news/xage-security-and-darktrace-partner-to-enhance-zero-trust-protection (дата звернення: 11.11.2024).

9. Shield Your Enterprise with Zero Trust Access from Xage. Xage Security. URL: https://xage.com/zero-trust-access/ (дата звернення: 13.11.2024).

10. Universal Zero Trust Network Access. Xage Security. URL: https://xage.com/universal-zero-trust-network-access/ (дата звернення: 13.11.2024).

11. Xage: Zero trust cybersecurity for IT, OT, and cloud. URL: https://xage.com/wp-content/uploads/2023/05/Xage-Zero-Trust-Data-Exchange.pdf?hsCtaTracking=78b2a2b1-6699-4a77-b034-22abbbcd4f46|322a397a-d05d-41c2-9f81-292ba926b3a0 (дата звернення: 15.11.2024).

12. Mastering MITRE ATT&CK for Enterprise with a Zero Trust Model. WHITEPAPER. Xage Security. 2024

13. Unified Zero Trust Access and Protection for Operational Technology (OT) and Cyber Physical Systems (CPS) WHITEPAPER. Xage Security. 2024