COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.155

УДК 004.75; 004.8

ПОКРАЩЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ОБМЕЖЕНИХ РЕСУРСІВ

Р. М. Сиротинський, І. Я. Тишик

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: Сиротинський Роман Михайлович <roman.m.syrotynskyi@lpnu.ua>,
Тишик Іван Ярославович <ivan.y.tyshyk@lpnu.ua>

©Сиротинський Р. М., Тишик І. Я., 2024

Розглянуто способи покращення безпеки мережевої інфраструктури підприємства в умовах сучасних викликів, основні етапи впровадження безпекових рішень, що дають змогу нівелювати потенційні вразливості системи та визначити можливі інформаційні втрати. Примітно, що глобальна цифровізація породжує розвиток нових технологій та підходів в інформаційній індустрії. Пристрої, механізми та аплікації, які раніше були автономними, стають вузлами глобальної інформаційної мережі. Така трансформація інформаційних технологій значно розширює ландшафт реалізації кіберзагроз. З кожним роком традиційні моделі безпеки комп'ютерних мереж втрачають свою актуальність, тому для їх захисту від сучасних кіберзагроз стає потребою розроблення та впровадження нових підходів, які б підвищували ефективність захисту інформаційних систем.

Проаналізовано потенційні вектори атак на мережеву інфраструктуру підприємства на основі традиційної моделі безпеки, розглянуто типові шляхи їх усунення, досліджено складові частини моделі безпеки Zero Trust Network Access та запропоновано низку заходів щодо підвищення стійкості мережевої інфраструктури підприємства до кіберзагроз.

Враховуючи сучасні тенденції поширення кіберзагроз та проведеного аналізу вибраних заходів їх протидії, визначено критичність реалізації загроз кожному з пропрацьованих шляхів підвищення рівня захищеності мережевої інфраструктури підприємства та запропоновано послідовність їх впровадження з урахуванням складності реалізації її захисту за обмежених ресурсів підприємства.

Ключові слова: комп'ютерна мережа, мікросегментація, архітектура Zero Trust Network Access, кіберзагроза, периметер безпеки.

Вступ

Очевидно, що світ цифрових технологій є не лише новим логічним етапом розвитку технологічної сфери людства, а все більше входить в роль одного з основних гравців економічної, соціальної, культурної, освітньої та інших, здавалося б, малопов'язаних з технологіями, сфер людства. Наразі ще не визначені загальноприйняті та усталені дефініції чи юридичні визначення, однак, з кожним роком цифрові технології все глибше проникають майже у всі сфери життя суспільства. Цифровізація (англ. *digitalization*) стає найважливішим фактором економічного зростання будь-якої країни і взагалі є сучасним трендом розвитку [1]. Саме цей процес спостерігається останні 5–10 років майже у кожному підприємстві, закладі чи установі, які здійснюють

опрацювання різного виду інформації, надають ті чи інші цифрові послуги або використовують сучасні послуги, сервіси чи технології.

Цифровізація бізнесу у поєднанні з останніми тенденціями впровадження віддаленої роботи, використання гібридних та хмарних середовищ, а також засилля різного роду цифрових розумних пристроїв потребує нових підходів та інвестицій в інформаційну безпеку. Класичні моделі та методи мережевої безпеки на основі периметра стають малоефективними, оскільки типовий, легко ідентифікований периметр безпеки стає надто вразливим до різного виду кіберзагроз. Периметроцентрична безпека мережі є також недостатньою, бо після потрапляння зловмисника всередину периметра безпеки, його зловмисні дії на "горизонтальному рівні" стають потенційно безперешкодними. Глобальна цифровізація та недостатні інвестиції в інформаційну безпеку зумовлюють підвищене зацікавлення кіберзлочинців здійсненням ними неправомірної діяльності щодо несанкціонованого втручання в роботу інформаційної системи підприємства. Така несанкціонована діяльність зазвичай призводить до матеріальних та репутаційних збитків цього підприємства.

Згідно з оцінками Cybersecurity Outlook від Statista, очікується, що глобальні витрати на кіберзлочинність різко зростуть у наступні п'ять років: від 8,44 трлн доларів у 2022 році до 23,84 трлн доларів до 2027 року. Журнал "Cyber Crime Magazine" визначає кіберзлочинність як "пошкодження та знищення даних, вкрадені гроші, втрата продуктивності, крадіжка інтелектуальної власності, крадіжка особистих і фінансових даних, розкрадання, шахрайство, порушення нормального ходу бізнесу після атаки, судове розслідування, відновлення та видалення зламаних даних і систем, а також репутаційна шкода" [2].

1. Огляд літературних джерел

Традиційні мережеві архітектури, спроєктовані з використанням основоположних моделей безпеки на базі периметра, стикаються з численними складними та унікальними проблемами в епоху сучасних цифрових технологій. Розвиток кіберзагроз і складність методології виявлення атак демонструють значні вразливості у таких традиційних мережевих структурах. У цьому розділі досліджено сучасні вразливості класичних мереж, підкреслено потребу вдосконалених заходів безпеки та зміни парадигми до стійкіших мережевих моделей, таких як Zero Trust.

Згідно з дослідженнями, пейзаж кіберзагроз істотно змінився, кіберзлочинці використовують найновіші підходи та засоби для експлуатації вразливостей корпоративних мереж. Корпоративні інформаційні мережі, які часто побудовані за принципом організації периметру безпеки для захисту внутрішніх даних, систем та ресурсів, недостатньо орієнтовані для протидії динамічній природі теперішніх кіберзагроз. Шкідливе програмне забезпечення, додатки-вимагачі, фішинг, а також розвинені сталі загрози (APT) стали складнішими, що дає змогу їм порівняно легко обходити традиційні засоби безпеки. Наприклад, APT – це високоспеціалізовані та складні атаки, ретельно розроблені для націлювання на конкретну компанію чи організацію. Ці атаки важче запобігти, виявити та пом'якшити, оскільки вони розроблені для ухилення від заходів безпеки, доступних у цільовій організації. Такі атаки містять не лише різноманітні інструменти, а й різні тактики та техніки [3].

Згідно з результатами досліджень, одними з найбільш типових вразливостей у класичних мережах є:

Порушення периметра безпеки: класично побудовані мережі часто покладаються на брандмауери та системи виявлення вторгнень для захисту своїх периметрів. Однак як тільки ці периметри порушено, зловмисники можуть переміщатися у мережі з невеликим опором, використовуючи внутрішні її ресурси [4].

Інсайдерські загрози: інсайдерські загрози становлять значний ризик для класичних мереж. Зловмисні інсайдери або скомпрометовані облікові дані користувача можуть призвести до витоку даних, крадіжки інтелектуальної власності та саботажу, використовуючи неявну довіру всередині мережі [5].

Невиправлені системи та вразливості програмного забезпечення: класичним мережам часто важко підтримувати оновлені системи та програми. Неоновлені системи безпеки стають вразливими, оскільки є потенційними цілями для зловмисників, даючи змогу їм використовувати застаріле програмне забезпечення та отримувати несанкціонований доступ до мережевих ресурсів [6].

Для боротьби з цими вразливостями запропоновано кілька сучасних рішень і підходів, які були прийняті багатьма організаціями:

Архітектура нульової довіри: нульова довіра – це концепція безпеки, яка будується на твердженні, що будь-що всередині чи за межами організації не має автоматично бути довіреним, а натомість, треба перевіряти все, що намагається під'єднатися до корпоративних систем, перш ніж йому буде наданий доступ. Цей підхід мінімізує бічний рух і забезпечує надійний захист від внутрішніх і зовнішніх загроз [7].

Мікросегментація: впровадження мікросегментації дає змогу поділити мережу на дрібніші, більш керовані сегменти мережі, які мають власні елементи керування безпекою. Ця стратегія обмежує здатність зловмисника переміщатися всередині мережі та локалізувати потенційні порушення в ізольованих сегментах [8].

Регулярне керування виправленнями та оцінка вразливостей: впровадження процесу моніторингу інформаційної системи після внесення у неї змін та проведення регулярних оцінок вразливостей її активів може значно знизити ризик несанкціонованого втручання. Автоматизовані інструменти та спеціалізовані групи кібербезпеки відіграють вирішальну роль у швидкому виявленні та виправленні вразливостей [9].

Інші дослідження твердять, що є чимало труднощів, з якими доведеться зіткнутися в разі імплементації вказаних підходів. Однією з головних проблем впровадження архітектури мережі з нульовою довірою, згідно з твердженням спільноти LinkedIn, є складність проєктування, розгортання та керування нею [10]. Треба визначити детальну політику для кожного ресурсу, сегментувати свою мережу на мікропериметри та постійно контролювати весь трафік і активність. Також потрібно інтегрувати кілька інструментів і технологій, таких як ідентифікація та керування доступом, шифрування, захист кінцевої точки та мережеві брандмауери. Всі ці завдання є складними в реалізації, потребують якісної координації та є ресурсозатратними.

Іншим не менш важливим та неминучим викликом впровадження засобів захисту інформації з архітектури нульової довіри є висока витратна вартість як наслідок складності впровадження разом із проблемою несумісності застарілих засобів та технологій з новими вимогами та задачами, які мусять підтримуватися та бути розв'язаними. Ця проблема провокує нові задачі для досягнення та вирішення оптимального та найбільш ефективного підходу (послідовності) впровадження архітектури нульової довіри в інформаційній інфраструктурі підприємства.

2. Постановка завдання

Приймаючи те, що традиційні моделі безпеки комп'ютерних мереж поступово втрачають свою актуальність, постає потреба у розробленні та впровадженні нових підходів, які б підвищували ефективність захисту інформаційних систем від сучасних кіберзагроз загалом. З огляду на сказане, актуальним завданням роботи є пошук способів покращення безпеки традиційної корпоративної мережі, підвищення ефективності захисту її операційних середовищ, даних та вузлів з урахуванням вимог захисту сучасних корпоративних сервісів та продуктів, а також запропонувати найефективніші шляхи їх реалізації з урахуванням складності впровадження та обмежених ресурсів, виділених на імплементацію цих засобів та заходів.

3. Виклад основного матеріалу дослідження

Типова комп'ютерна мережа підприємства розв'язує певний перелік задач, які виникають під час побудови корпоративної інфраструктури цього підприємства. Найпоширенішими потребами є дротове та бездротове під'єднання клієнтських комп'ютерів та мобільних пристроїв, зазвичай

дротове підключення серверів, які обслуговують корпоративні віртуальні машини, під'єднання мережі до інтернету та можливість обмінюватися даними між комп'ютерами та серверами, а також спільний доступ обох груп в інтернет і повне блокування запитів, ініційованих з інтернету всередину мережі до вузлів, які там розміщені. Винятком може бути потреба організації публічного доступу з інтернету для систем, розміщених на серверній інфраструктурі підприємства. В такому разі такий доступ реалізовується методом винесення відповідних серверів за периметр безпеки в так звану демілітаризовану зону, доступ до якої регулюється політиками безпеки на корпоративному файрволі. Якщо підприємство розміщується в декількох географічно розділених локаціях, то потреба в мережевому з'єднанні вирішується або виділеною лінією на базі оптичних волокон, або VPN під'єднаннями на кшталт сайт до сайту на базі VPN шлюзів чи файрволів через публічну інтернет-мережу.

Трансформація корпоративних сервісів, спричинена пандемією COVID19, найвірогідніше, сформувала ще одну задачу, яка стала вже базовою сьогодні – потребу віддаленого під'єднання працівників до своїх робочих місць чи до корпоративних ресурсів з-за меж периметра корпоративної мережі. Цю задачу типово розв'язують одним з багатьох рішень віддаленого доступу, які працюють на базі клієнтського VPN під'єднання до корпоративного файрвола чи VPN концентратора. VPN використовується для зменшення ризику втрати внутрішніх даних, полегшення роботи віддаленої робочої сили та захисту від зловмисних атак [11].

Описаного функціоналу могло б бути достатньо років з 10 назад, коли кількість кіберзлочинів та несанкціонованих проникнень в корпоративну мережу була в рази нижча, ресурси які виділялися на мережеву безпеку були істотно менші, а кіберзлочинці були не настільки майстерними, як сьогодні.

Традиційна мережева безпека на основі периметра сьогодні все частіше вважається недостатньою з кількох причин, спричинених змінами в технологічному ландшафті, розвитком кіберзагроз і новими способами роботи. Нижче наведено основні причини, підтверджені наявними практиками та напрацюваннями, а також науковими та галузевими дослідженнями:

Еволюція ландшафту загроз: традиційні моделі безпеки ґрунтуються на припущенні, що загрози є переважно зовнішніми. Однак сучасний ландшафт загроз становить складні кіберзагрози, які можуть виникати як ззовні, так і всередині мережі, зокрема внутрішні загрози, розвинені сталі загрози (APT) і зловмисне програмне забезпечення, яке може обходити захист периметра.

Горизонтальний рух в мережі: одразу після проникнення в мережу на базі периметроцентричної моделі безпеки кіберзлочинець має змогу безперешкодно рухатися горизонтально та інфікувати сусідні системи чи проникати в сусідні підмережі. Такій моделі зазвичай не вистачає інструментів та засобів контролю внутрішнього обміну даними, що дає змогу зловмисникам інфікувати сусідні системи, переміщатися непоміченими всередині периметра безпеки та безперешкодно добиратися до конфіденційних даних і систем.

Обчислення в хмарах та мобільні робочі групи: перехід до обчислень в хмарах і поширеність віддаленої роботи зруйнували традиційні мережеві кордони. Оскільки корпоративні аплікації і дані тепер хостяться в хмарах та доступ до них відбувається з різних пристроїв і локацій віддалено, то підхід чітко визначеного периметра безпеки мережі більше не може бути використаний. Така кооперація потребує підходів безпеки, які опікуються захистом даних без прив'язки до того, де вони зберігаються чи де до них відбувається доступ.

Потреба в нульовій довірі: недостатня захищеність традиційної моделі безпеки, орієнтованої на периметр, акцентує важливість застосування моделі безпеки з нульовою довірою. Zero Trust діє за принципом "ніколи не довіряй, завжди перевіряй", застосовуючи сувору перевірку особи і контроль доступу для кожного користувача та пристрою, як у мережі, так і поза нею, щоб мінімізувати поверхню атаки та зменшити ризик злому [12].

Інтернет речей (IoT): різке збільшення кількості пристроїв IoT значно розширює кількість точок входу в мережу. Значна кількість IoT пристроїв не має достатніх засобів безпеки, що знижує їхню стійкість до сучасних атак. Традиційні безпекові підходи на основі периметра не

передбачають масштаб і різноманіття пристроїв IoT. Як наслідок, мережі залишаються потенційно вразливими до зловмисного проникнення з використанням скомпрометованих IoT пристроїв.

Для модифікації корпоративної мережі, побудованої за традиційним підходом, і покращення рівня захищеності від актуальних загроз розглянемо певні безпекові заходи на шляху до моделі безпеки "Мережевий доступ нульової довіри" (ZTNA) .

Zero Trust Network Access (ZTNA) – це безпекова модель та комплекс технологій, які в роботі послуговуються принципом "ніколи не довіряй, кожного разу перевіряй". На противагу традиційним безпековим моделям, які вважають, що все, що вже потрапило всередину мережі, є безпечним, ZTNA первинно стверджує, що всі користувачі і пристрої є потенційною загрозою, не беручи до уваги, де вони розміщуються: в периметрі мережі чи поза ним. Доступ до мережевих ресурсів надається на основі суворої перевірки особи, мінімальних прав доступу та постійного моніторингу поведінки користувачів і стану безпеки пристрою. Метою ZTNA є надання безпечного віддаленого доступу до програм і даних, зниження ризику витоку даних та інших кіберзагроз, забезпечуючи доступ до мережевих ресурсів лише автентифікованим і авторизованим користувачам і пристроям [13].

Zero Trust Network Access (ZTNA) є частиною ширшої моделі безпеки Zero Trust. Zero Trust – це стратегічний підхід до кібербезпеки, який діє за принципом "ніколи не довіряй, постійно перевіряй". На противагу традиційним моделям безпеки, що зазвичай вважають все всередині мережі організації безпечним, Zero Trust припускає, що загрози можуть надходити з будь-якого місця – як ззовні, так і всередині мережі – і, отже, жодному користувачеві чи пристрою не можна довіряти за замовчанням. Ця модель потребує суворої перевірки ідентифікації, мінімальних дозволів доступу та постійного моніторингу всіх користувачів і пристроїв, незалежно від того, намагаються вони отримати доступ до ресурсів у межах периметра мережі чи з віддалених місць.

Шлях до впровадження моделі Zero Trust Network Access є трудомістким та затратним. Деякі постачальники позиціонують свої продукти як рішення ZTNA з коробки, тобто такі, що не потребують значних втручань чи затрат на впровадження та операційну підтримку. Це або неправда, або рішення на базі таких продуктів будуть негнучкими чи неефективними.

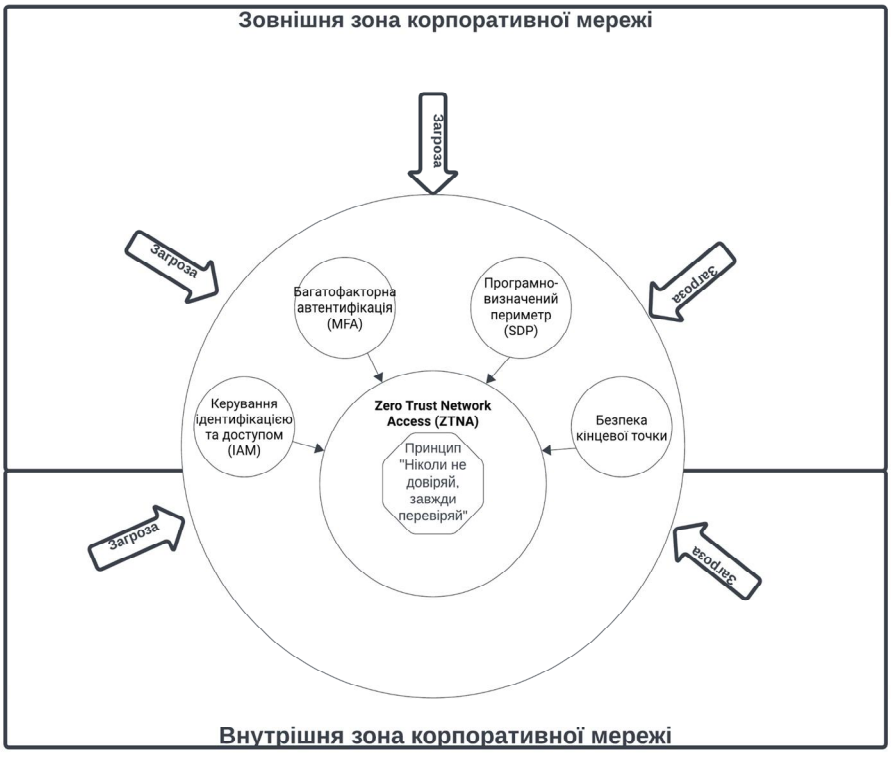

Рис. 1. Концепція моделі безпеки Zero Trust Network Access

Аналогічно до стовпів моделі зрілості Zero Trust, впровадження елементів ZeroTrust Network Access є поступовим і індивідуальним залежно від інфраструктури підприємства. Є певні початкові етапи, проміжні та завершальні заходи, які формують модель зрілості цієї архітектури. Оптимальна послідовність їх впровадження з урахуванням індивідуальної інфраструктури певного підприємства та конкретних можливостей інвестування в цю ініціативу має бути розрахована та визначена задля створення найбільш ефективної дорожньої карти реалізації безпекової ініціативи.

Щоб успішно реалізувати та отримувати всі переваги вказаного підходу, навіть за умови купівлі спеціалізованого рішення, передбачається певна організаційна та оцінна робота перед зміною та застосуванням оновлених політик безпеки та безпечного доступу, а також систематична операційна робота з перегляду та контролю налаштувань після імплементації, що своєю чергою створює певне операційне навантаження на обслуговувальний персонал. Бізнес має визначити випадки використання “користувач-додаток-дані”, де ZTNA матиме найбільший вплив (наприклад, контроль доступу до конфіденційних програм і даних або надання доступу для певних груп користувачів, наприклад підрядники). Він також має застосовувати спеціальні політики до відповідних сфер діяльності, де потрібен безпечний доступ.

На заміну VPN віддаленого доступу зазвичай розгортається мережевий доступ із нульовою довірою, але надто складні політики перешкоджають прийняттю. Щоб досягти успіху, лідери з питань безпеки та управління ризиками мають прийняти підхід безперервного життєвого циклу до управління віддаленим доступом [14] – стверджує Gartner, Inc, компанія, яка виступає як лідер у галузі консультацій та аналітики в сфері IT у своєму звіті про сім ефективних кроків для впровадження доступу до мережі з нульовою довірою.

Розглянемо основні етапи підвищення безпеки мережевої інфраструктури підприємства впровадженням безпекових заходів з методології ZTNA та проведемо орієнтовну оцінку затрат на впровадження та операційну підтримку.

1. **Аналіз мережевих потоків даних та важливих корпоративних аплікацій**. Одним з важливих початкових етапів має бути аналіз наявних під’єднань в мережі, список користувачів та критично важливих бізнесу аплікацій. Вичерпний перелік таких з’єднань та сутностей окреслить той потрібний набір політик безпеки, який буде формувати та дозволяти саме легітимний трафік, а всі інші з’єднання мають заборонятися.

2. **Багатофакторна автентифікація**: MFA – це метод захисту облікових даних користувача, який потребує надання двох або більше форм доказу своєї ідентичності для доступу. Є достатньо багато варіантів організації додаткового фактора автентифікації, популярними є використання апаратних ключів (токенів), отримання коду в текстовому повідомленні на мобільний номер, а також підтвердження другого фактору в додатку на мобільному пристрої.

3. **Контроль доступу та ідентичностей (IAM)**: потрібен для контролю ідентичності всіх користувачів та пристроїв, які намагаються створити з’єднання до мережевих ресурсів. Системи IAM забезпечують доступ до певних програм і даних лише для автентифікованих і авторизованих користувачів. Існує два типи сутностей, які потрібно автентифіковувати: користувач та нелюдська ідентичність, чи NHI (зазвичай скрипти та аплікації). Ці сутності можуть приходити в мережу з різних місць, і сукупність систем IAM мають вміти автентифіковувати користувачів та некористувачів в усіх можливих точках входу.

4. **Мікросегментація**: розділяє мережу на безпечні зони для контролю доступу та пересування в мережі. Мікросегментація допомагає обмежити здатність зловмисника переміщатися мережею за допомогою застосування суворого контролю доступу до кожного сегмента. В певних випадках може частково компенсовувати брак механізму IAM на некористувачах, за умови, що на одну зону чи інтерфейс припадає одна аплікація, тоді її ідентичність окреслюється, власне, її унікальною адресацією.

5. **Доступ з мінімальними привілеями**: забезпечує надання мінімально достатнього рівня доступу чи дозволу для користувачів та пристроїв, який потрібний для розв’язання поставлених завдань, водночас мінімізуючи ймовірний рівень взлому. За великої кількості користувачів допускається деяке узагальнення, за умови, що цільова система не є критичною аплікацією, заради

зниження операційного навантаження з керуванням доступів. За такого підходу балансування між операційним навантаженням та гарантуванням безпеки приймається індивідуально, беручи до уваги рівень ресурсів, доступних на операційне навантаження.

Рішення стосовно балансу між безпекою та операційним навантаженням приймається з урахуванням виділених ресурсів на останнє.

6. **Постійний моніторинг безпеки та аналітика:** передбачає неперервне вивчення мережевого трафіку, дій користувачів та підозрілих подій з метою ідентифікації та миттєвого реагування на постійні загрози. Ця компонента є критично важливою в процесі ідентифікації аномальних подій, наявність яких може трактуватися як факт зловмисного втручання в безпеку. Критично значущим в реалізації цього етапу є потреба переходу від ручного до максимально автоматизованого процесу моніторингу та аналізу для пришвидшення реакції на нетипову подію чи аномалію та зниження ймовірності людської помилки під час ручного опрацювання інформації.

7. **Захист кінцевих вузлів**. Захист кінцевих вузлів є надзвичайно важливим у межах Zero Trust Network Access, концентруючись на безпеці пристроїв, які під'єднуються і працюють в мережі. Він забезпечує кожному пристрою автентифікацію, захист від зловмисного програмного забезпечення та відповідність сучасним стандартам безпеки під час під'єднання до мережі та взаємодії з її ресурсами, використовуючи такі технології, як автентифікація пристрою, перевірка відповідності кінцевих точок: оцінка стану безпеки пристрою, вакож версія його операційної системи, рівень виправлення та наявність потрібного програмного гарантування безпеки (антивірус, брандмауери тощо). Пристроям, які не проходять перевірку на відповідність визначеним безпековим критеріям, можна обмежити доступ та помістити в сегмент мережі з доступом лише на мінімальні корпоративні ресурси.

8. **Шифрування:** гарантує безпеку даних у процесі їх трансляції та збереження, виключаючи можливість доступу до конфіденційної інформації для несанкціонованих осіб чи пристроїв. Задачу шифрування даних можна перенести на аплікаційний рівень, а в контексті мереж додаткове шифрування трафіку варто реалізовувати, де інформація виходить за межі фізичного периметру безпеки, навіть якщо це орендований виділений канал.

9. **Рішення Software-Defined Perimeter (SDP)/Zero Trust Network Access (ZTNA)**: рішення SDP/ZTNA створюють безмежний, динамічний і безпечний механізм контролю доступу до мережі, який працює за принципом "ніколи не довіряй, завжди перевіряй". SDP – це нова технологія доступу до програми, яка використовується для автентифікації користувачів, авторизації прав доступу до програми на основі профілів користувачів, а також виконує постійну оцінку ризиків упродовж сеансу. Це рішення в більшій частині випадків не є сумісним із застарілим мережевим обладнанням і потребує повного оновлення стеку обладнання традиційної корпоративної мережі та перегляду архітектури її побудови.

4. Результати досліджень

За номінальну мережеву інфраструктуру візьмемо мережу, яка складається з файрвола, двох свічів та корпоративного сервера – гіпервізора з певною кількістю віртуальних машин з різними ролями. Для користувачів доступна робота з офісу та віддалене під'єднання засобами ВПН.

Заходи забезпечення підвищення рівня безпеки мережевої інфраструктури, перелічені вище, зареєструємо в таблиці. Визначення експертної оцінки щодо трудозатратності впровадження відбудеться з врахуванням технічної складності впровадження певних заходів та потреби кваліфікованого персоналу. На оцінку вартості програмно апаратних продуктів, потрібних для забезпечення кроків підвищення безпеки мережі, буде впливати їхня орієнтовна вартість на ринку.

Пріоритетність впровадження компонентів Zero Trust Network Access (ZTNA) з огляду на глобальну статистику хакерських і кіберзагроз передбачає зосередження насамперед на областях, які найчастіше використовуються зловмисниками. На основі останніх звітів [15, 16, 17] про кіберзагрози та тенденцій пропонується порядок впровадження кроків підвищення безпеки мережі, який записаний в таблиці в порядку спадання від найбільш вагомого. Відповідно до позиції внесемо їх ваговий коефіцієнт критичності.

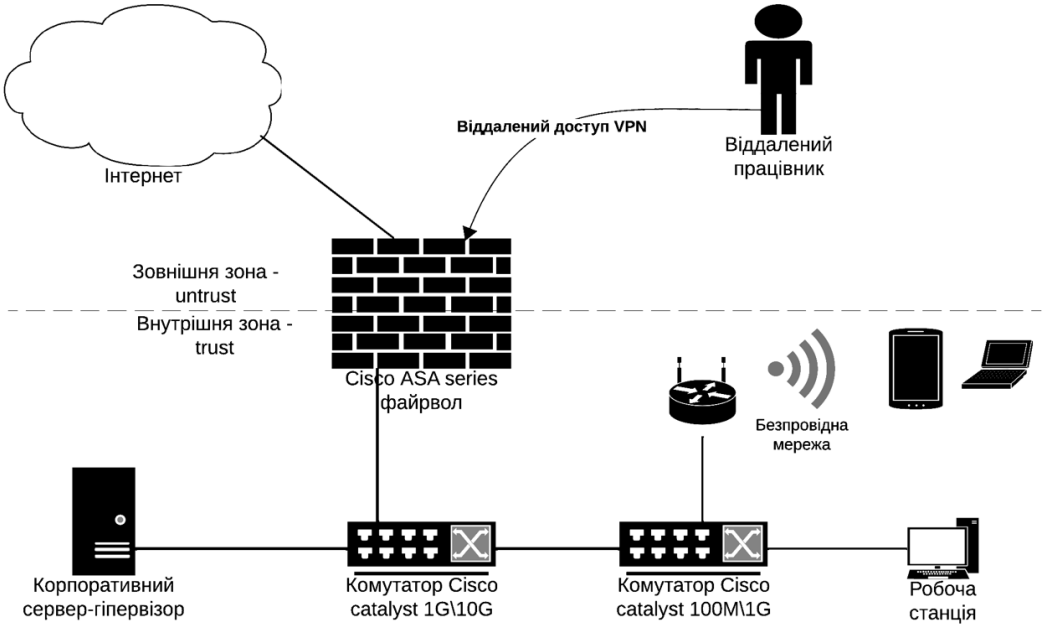

Рис. 2. Топологія традиційної мережі моделі безпеки на базі периметру

Таблиця оцінки критичності та складності впровадження рішень

Способи підвищення безпеки мережі	Коефіцієнт критичності, [k]	Трудозатратність впровадження 3 – низька 2 – середня 1 – висока, [c]	Потреба в платних рішеннях 3 – не потребує 2 – ціна < 1000 $ 1 – ціна > 1000 $ [m]	Кінцева оцінка x * (y+z) [F]	Коментар
Багатофакторна автентифікація (MFA)	8	2	2	32	
Аналіз під'єднань та аплікацій	7	2	3	35	
Управління ідентифікацією та доступом (IAM)	6	2	2	24	
Контроль доступу з найменшими привілеями	5	2	3	25	
Безпека кінцевої точки	4	2	2	16	
Мікросегментація мереж	4	2	1	12	Мікросегментація потребує дорогого мережевого екрану
Безперервний моніторинг і аналітика безпеки	3	1	1	6	Ефективні SIEM аплікації є комерційними
Шифрування	2	2	2	8	
Засоби Software-Defined Perimeter (SDP) для ZTNA	1	1	1	2	Рішення базовані на SDP є і дороговартісними і складними

Критерій оптимальності для послідовності підвищення безпеки мережевої інфраструктури підприємства визначається як комплексна оцінка, отримана за допомогою обчислення добутку коефіцієнта критичності та суми експертних оцінок з трудозатратності на впровадження та потреби використання платних програмних чи апаратних продуктів. Оцінка критерію оптимальності (F) має вигляд:

$$F = k * (c + m) \rightarrow max \quad . \qquad (1)$$

Відсортувавши результати обчислень від більшого до меншого, отримаємо рекомендовану послідовність заходів, які потрібно впровадити для підвищення стійкості мережевої інфраструктури підприємства до сучасних кіберзагроз, за умови обмежених ресурсів на їх реалізацію.

Висновки

У цьому дослідженні проаналізовано динаміку та вплив зростання цифровізації в світі на горизонт кіберзагроз. Визначено нові виклики до безпекової моделі комп'ютерної мережі підприємства, які не покриваються при традиційному підході та потребують впровадження нових засобів та заходів мережевої безпеки для підвищення стійкості до сучасних кібератак.

Визначено способи підвищення безпеки мережевої інфраструктури підприємства та запропоновано оптимальну послідовність їх впровадження з урахуванням пріоритетності розв'язуваної задачі, складності реалізації та обмежених ресурсів.

На основі отриманих результатів встановлено, що насамперед варто впроваджувати заходи з найменшими затратами на впровадження та найбільш вагомим коефіцієнтом критичності, а за накопиченням відповідних ресурсів переходити до наступних кроків. Треба зауважити, що результати цього дослідження не знецінюють важливості застосування заходів з кінцевим нижчим балом, а лише мають рекомендаційний характер, залежно від послідовності їх виконання, коли немає змоги впроваджувати одночасно декілька з них, чи усі разом.

Перспективи подальших досліджень можуть бути спрямовані на розробку підходів щодо підвищення ефективності захисту інформаційної системи підприємства загалом з урахуванням коректного впровадження сучасних корпоративних сервісів, комунікаційного обладнання та програмних продуктів, практичної реалізації безпекових елементів корпоративної мережі для захисту від кіберзагроз.

Список літератури

1. Sosnin O. (2020). Cyfrovizaciya yak nova realnist` Ukrayiny. Lex. Inform. [Digitization as a new reality of Ukraine] Retrieved from: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ [In Ukrainian] (Accessed: 15 March 2024).

2. Fleck A. (2024, February 22). Cybercrime Expected To Skyrocket in Coming Years. Retrieved from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027 (Accessed: 26 February 2024).

3. Ashwini Kumari M. and Nandini Prasad K. S. A Behavioral Study of Advanced Security Attacks in Enterprise Networks, 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2021, pp. 1–5. DOI: 10.1109/CSITSS54238.2021.9682903

4. Anjum I., Kostecki D., Leba E., Sokal J., Bharambe R., Enck W., Nita-Rotaru C., & Reaves B. (2022). Removing the Reliance on Perimeters for Security using Network Views. Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies. pp. 151–162, https://doi.org/10.1145/3532105.3535029

5. Sheikh N., Pawar M., & Lawrence V. (2021). Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

6. Wu Y. G., Yan W. H. and Wang J. Z. Real identity based access control technology under zero trust architecture, 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 2021, pp. 18–22, doi: 10.1109/ICWCSG53609.2021.00011

7. Nair Anita (2021). The Why and How of adopting Zero Trust Model in Organizations. TechRxiv. Preprint. pp. 1–6, https://doi.org/10.36227/techrxiv.14184671.v1

8. Hines C. D. and Chowdhury M. M. Uncover Security Weakness Before the Attacker Through Penetration Testing, 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 492–497, doi: 10.1109/eIT53891.2022.9813950

9. Abhishek Arote, Umakant Mandawkar. Android Hacking in Kali Linux Using Metasploit Framework, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp. 497–504, May–June-2021. Available at doi: https://doi.org/10.32628/CSEIT2173111

10. What are the main challenges and benefits of implementing a zero trust network architecture? (2023, October 6). Retrieved from https://www.linkedin.com/advice/1/what-main-challenges-benefits-implementing-4e (Accessed: 26 February 2024).

11. Tyshyk I. (2023). Vybir tekhnolohii viddalenoho dostupu dlia efektyvnoi orhanizatsii zakhystu merezhevykh ziednan. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", 3(19), pp. 34–45. DOI: 10.28925/2663-4023.2023.19.3445

12. Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma. A Survey on Zero Trust Architecture: Challenges and Future Trends, Wireless Communications and Mobile Computing, vol. 2022, Article ID 6476274, 13 pages, 2022. https://doi.org/10.1155/2022/6476274

13. Rose S., Borchert O., Mitchell S., & Connelly S. (2020). Zero Trust Architecture. NIST Special Publication 800–207. National Institute of Standards and Technology. pp. 1–50, DOI: 10.6028/NIST.SP.800-207

14. Koeppen D., MacDonald N., Watts J. (2022, October 3). 7 Effective Steps for Implementing Zero Trust Network Access. Retrieved from: https://emt.gartnerweb.com/ngw/eventassets/en/conferences/hub/identity-access-management/documents/gartner-iam-implementing-zero-trust-network-access.pdf (Accessed: 26 February 2024).

15. Deloitte Cybersecurity Threat Trends Report 2023. (n.d.). Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2023.html (Accessed: 26 February 2024).

16. M-Trends 2023: Cybersecurity Insights From the Frontlines, Mandiant. Report. Retrieved from: https://www.mandiant.com/resources/blog/m-trends-2023 (Accessed: 26 February 2024).

17. The 2024 SonicWall Cyber Threat Report, SonicWall, 2024, Retrieved from: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf (Accessed: 26 February 2024).

IMPROVEMENT THE SECURITY OF THE ENTERPRISE'S NETWORK INFRASTRUCTURE IN CONDITIONS OF MODERN CHALLENGES AND LIMITED RESOURCES

R. Syrotynskyi, I. Tyshyk

Lviv Polytechnic National University,
Department of Information Protection

© Syrotynskyi R., Tyshyk I., 2024

Ways to improve the security of the enterprise's network infrastructure in the face of modern challenges, the main stages of the implementation of security solutions, which makes it possible to eliminate potential system vulnerabilities and determine possible information losses, are considered. It is noteworthy that global digitalization gives rise to the development of new technologies and approaches in the information industry. Devices, mechanisms and applications that were previously autonomous are becoming nodes of a global information network. Such a transformation of information technologies significantly expands the landscape of the implementation of cyber threats. Every year, traditional models of computer network security lose their relevance, therefore, in order to protect them from modern cyber threats, it becomes necessary to develop and implement new approaches that would increase the effectiveness of the protection of information systems.

Potential vectors of attacks on the network infrastructure of the enterprise based on the traditional security model were analyzed, typical ways to eliminate them were considered, the components of the Zero Trust Network Access security model were studied, and a number of measures were proposed to increase the resistance of the enterprise network infrastructure to cyber threats.

Taking into account the current trends in the spread of cyber threats and the analysis of selected measures to counter them, the criticality of threat implementation is determined for each of the developed ways of increasing the level of security of the enterprise's network infrastructure, and the sequence of their implementation is proposed, taking into account the complexity of implementing its protection with limited enterprise resources.

Keywords: computer network, micro-segmentation, Zero Trust Network Access architecture, cyber threat, security perimeter.