Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Дослідження процесу організації зонової безпеки у комп'ютерній мережі**

Виконав(ла): курсу 6, груп и СНнм-61
студент(ка) спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

Федина В.В.
(підпис) (прізвище та ініціали)

Керівник Гром'як Р.С.
(підпис) (прізвище та ініціали)

Нормоконтроль Мацюк О.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент Жаровський Р.О.
(підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня МАГІСТР
(назва освітнього ступеня)

за спеціальністю 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

студенту Федині Владиславу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи **Дослідження процесу організації зонової безпеки у комп'ютерній мережі**

Керівник роботи **Гром'як Роман Сильвестрович, к.ф.-м.н., доц.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « » 20___ року № .

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічне завдання на дослідження процесу організації зонової безпеки у комп'ютерній мережі

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області; 2 Методи та засоби організації зонової безпеки в комп'ютерній мережі; 3 Охорона праці та безпека в надзвичайних ситуаціях; Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета, об'єкт предмет дослідження; Завдання дослідження; Модель захисту мережі на основі власного IT відділу; Модель захисту мережі з залученням зовнішніх фахівців; Модель захисту мережі на основі хмарних технологій; Логічна архітектура захисту мережі; Рішення Cisco для Secure access service edge (SASE); Реалізація Zero Trust Network Access (ZTNA); Захист мережі на основі брандмауерів (FireWall); Зміна методів автентифікації 2019-2021; Покращення автентифікації через використання безпарольного входу 2019-2021; Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Дмитроца Л.П., доц. каф. КН		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст.викл. каф ОХ		

7. Дата видачі завдання _____

1.1 КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	**1.2** Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи		*Виконано*
2.	Підбір наукових джерел щодо дослідження процесу		*Виконано*
	організації зонової безпеки комп'ютерної мережі		
3.	Переклад та опрацювання наукових джерел щодо		*Виконано*
	організації зонової безпеки комп'ютерної мережі		
4.	Виконання дослідження щодо процесів		*Виконано*
	організації зонової безпеки комп'ютерної мережі		
5.	Оформлення розділу «Аналіз предметної області»		*Виконано*
6.	Оформлення розділу «Методи та засоби організації		*Виконано*
	зонової безпеки в комп'ютерній мережі		
7.	Виконання завдання до підрозділу «Охорона праці»		*Виконано*
8.	Виконання завдання до підрозділу «Безпека в		*Виконано*
	надзвичайних ситуаціях»		
9.	Оформлення кваліфікаційної роботи		*Виконано*
10.	Нормоконтроль		*Виконано*
11.	Перевірка на плагіат		*Виконано*
12.	Попередній захист кваліфікаційної роботи		*Виконано*
13.	Захист кваліфікаційної роботи		

Студент _____ Федина В.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Гром'як Р. С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження процесу організації зонової безпеки у комп’ютерній мережі // Кваліфікаційна робота // Федина Владислав Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНнм–61 // Тернопіль, 2022 // С. 70 , рис. – 14 , табл. – , кресл. – , додат. – 4 , бібліогр. – 63 .

Ключові слова: БЕЗПЕКА, ЗОНИ БЕЗПЕКИ, БРАНДМАУЕР, АРХІТЕКТУРА БЕЗПЕКИ, ЗАГРОЗИ.

У роботі виконано дослідження процесу організації зонової безпеки у комп’ютерній мережі, що дало змогу розробити методи та засоби організації комплексного захисту мереж на основі зон з використанням сучасних технологій та підходів.

Перший розділ кваліфікаційної роботи висвітлює організацію розробки та будови мережі через впровадження точок входу в мережу з подальшим їх контролем та захистом, проаналізовано типи мережевих потоків даних для визначення нормального виду мережі, зійснено аналіз рівневого кіберзахисту.

Другий розділ кваліфікаційної роботи присвячений організації зонової безпеки комп’ютерної мережі. Подано основні архітектурні рішення забезпечення захисту мережі на основі зон.

Метою дослідження є процес організації зонової безпеки у комп’ютерній мережі. Об’єкт дослідження – процес передавання, та захисту інформації в мережах. Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

ANNOTATION

Study of the process of zone security organization in a computer network // Diploma thesis Master degree // Fedyna Vladyslav V. // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2022 // P. 70 , Tables – , Fig. – 14 , Diagrams – , Annexes. – 4 , References – 63 .

The research of the process of organization of zone security in the computer network is carried out in the work, which allowed to develop methods and means of networks complex protection organization on the basis of zones with the use of modern technologies and approaches.

The first section of the qualification work covers the organization of network development and construction through the introduction of network entry points with their subsequent control and protection, analyzed the types of network data flows to determine the normal type of network trafic, analysis of level cybersecurity is carried out.

The second section of the qualification work is devoted to the organization of zone security of the computer network. The main architectural solutions for network protection based on zones are presented.

The aim of the study is the process of organizing zone security in a computer network. The object of research is the process of transmitting and protecting information in networks. The subject of research is the theory of telecommunication networks design, data transmission theory, information protection theory.

Key words: SECURITY, SECURITY ZONES, FIREWALLS, SECURITY ARCHITECTURE, THREATS

ЗМІСТ

ВСТУП

Захист інформаційних ресурсів є ключовим фактором розвитку роботи організацій різного рівня. Правильно спроектована та захищена мережева інфраструктура забезпечує репутаційну вартість та створює комфортні умови для роботи персоналу та користувачів.

Швидкий розвиток методів та засобів організації захищених мереж зумовлений не менш швидкими темпами роботи хакерів. Кількість кібератак на інфраструктуру та ресурси мереж суттєво зросли за останні роки. Це приводить до пошуку нових рішень у виявленні та протидії загрозам сьогодення та майбутнього.

Актуальність теми. Дослідження процесу організації зонової безпеки у комп'ютерній мережі є важливим завданням, що дасть змогу розробити методи та засоби організації комплексного захисту мереж на основі зон з використанням сучасних технологій та підходів.

Мета і завдання дослідження. Метою дослідження є процес організації зонової безпеки у комп'ютерній мережі, що дасть змогу розробити або впровадити нові підходи, технології та моделі захисту мереж, забезпечити відслідковування змін у профілі поведінки мережі, зарповадити захист ключових вузлів, пристроїв та інформації. Досягнення поставленої мети передбачає виконання наступних завдань: здійснити аналіз визначення точок входу в мережу; виявити профілі типового трафіку; внести пропозиції щодо організації зонової безпеки мережі.

Об'єкт дослідження – процес передавання, та захисту інформації в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

Практичне значення одержаних результатів. Висвітлено організацію розробки та будови мережі через впровадження точок входу в мережу з

подальшим їх контролем та захистом, що дає змогу використовувати збільшений контроль у порівнянні з традиційними підходами. Проведено аналіз типів мережевих потоків даних для визначення нормального виду мережі, що уможливлює створення систем моніторингу за нетиповою роботою профілю мережевих ресурсів. Здійснено аналіз рівневого кіберзахисту, що показало можливість організації захисту даних на основі рівнів де кожен має свої вимоги до персоналу, наборів обладнання та вимог відповідності стандартам.

Наукова новизна розробки: проведено дослідження організації зонової безпеки комп’ютерної мережі. Подано індикатори вторгнення, що дають змогу на основі типових характеристик втручання розробляти відповідні методи та засоби захисту. Запропоновано використання глибокого тестування мережі для виявлення слабкостей та їх усунення. Подано основні архітектурні рішення забезпечення захисту мережі на основі зон. У логічній архітектурі узагальнено використання типових підходів організації безпечної роботи мережі. На основі досвіду провідних компаній показано комплексні міри та рішення організації зонової безпеки комп’ютерної мережі. Визначено роль хмарних сервісів в організації безпеки зон для різних сценаріїв. Запропоновано використання брандмауерів та надано рекомендації щодо впровадження даних засобів для їх ефективної роботи. Проведено аналіз можливості застосування методів підвищення захисту мереж на основі безпарольної автентифікації, що показує майбутні напрямки розвитку технології для забезпечення зонової безпеки критичних інфраструктур.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз визначення точок входу в мережу

Незалежно від типу організації існує ризик проблеми безпеки мережі. Через те що кожен бізнес має зв’язки із зовнішніми постачальниками виникає необхідність детально аналізувати ресурси організації та приймати міри щодо їх захисту [1-10].

Будь-яка відправна точка, що є зв’язком з невідомим ресурсом представляє потенційний ризик безпеки. Починаючи від спеціалізованого банківського обслуговування до постачальників послуг, внутрішній Wi-Fi відкриває ваші організації для зовнішнього світу і потребує вирішення проблем безпеки мережі.

Виникає необхідність вивчити необхідні кроки, щоб обмежити ризик таких проблем, а також як захистити вашу мережу та дані від хакерів, які ховаються за межами вашого периметра безпеки. Важливо створити основу безпеки, починаючи з рівня 1.

Проектування мережевої інфраструктури часто зосереджується безпосередньо на продуктивності – і не безпідставно. Продуктивність мережі – це те, що в кінцевому підсумку приносить гроші.

Суттєві втрати в вартості роботи можуть виникнути через невирішення проблем безпеки мережі, які призводять до вартісного порушення безпеки даних.

Продуктивність, безумовно, є критерієм вищого рівня і тому не має змоги розробити мережеву інфраструктуру без ретельної уваги до системи безпеки, яка починається з видимості мережі.

Місце розташування точок входу в мережу (ТВМ) багато в чому залежить від дизайну мережі та цілей безпеки. Наприклад, якщо найбільше турбує перешкоджання хакерам, існує потреба розмістити ТВМ за межами

свого брандмауера для моніторингу абонентів і LAN/WAN, а також вимірювання якості обслуговування та перевірки задоволення рівня сервісу.

Крім того існує потреба розміщення мережевих ТВМ всередині мережі та на її межі для підвищення захисту. Перший етап підтримує виявлення та запобігання вторгненням, а другий дає 100% видимість для брандмауера нового покоління та моніторингу пропускної здатності, запобігання витоку даних, а також аналізу протоколів і пакетів.

Розумна стратегія, незалежно від цілей, полягає в тому, щоб почати з виходу за межі мережі та працювати всередину. Перш за все потрібно створити периметр безпеки. Звідти розробляти дизайн для внутрішньої видимості.

Багато проблем із безпекою мережі пов’язані з внутрішніми проблемами, такими як неправильне або навмисне надсилання співробітниками важливої інформації з мережі. Тут рівень захисту даних відіграє важливу роль.

Невідповідність політиці безпеки стає все більшою витратою на проблеми з мережевою безпекою. Існує бажання мати можливість контролювати свої зони відповідності, щоб мати змогу бачити в реальному часі все, що відбувається у периметрі відповідності та аудиту. І єдиний спосіб забезпечити 100% видимість мережі – це використовувати мережеві ТВМ під час підключення пристроїв безпеки.

Якщо виникне загроза порушення та відбудеться втрата данних, записів чи інше, потрібно мати можливість довести керівним органам, що саме було втрачено.

Нове законодавство стверджує, що якщо немає змоги довести обмежену втрату записів, наприклад, п’ять записів із мільйона – слід вважати, що відбулась втрата усіх даних. Ця оцінка безпосередньо впливає на розмір штрафу за таких обставин.

У міру того, як відбувається просування вглиб мережі та ферм серверів, мережеві ТВМ відіграють важливу роль у забезпеченні абсолютного розуміння для аналізу продуктивності, усунення несправностей та оптимізації моніторингу продуктивності мережі та додатків.

1.2 Аналіз типового потоку даних мережі

Мережевий трафік – це кількість даних, які переміщуються по мережі протягом певного часу. Мережевий трафік також може називатися трафіком даних або просто трафіком [11-20].

У пошуковій оптимізації (SEO) трафік до мережі можна охарактеризувати як прямий, органічний або платний. Прямий трафік виникає, коли хтось вводить у браузер уніфікований локатор ресурсів (URL) веб-сайту. Органічний трафік – це прямий результат того, що хтось використовує пошукову систему для пошуку вмісту, а платний трафік означає, що хтось натиснув спонсоровану рекламу.

У адмініструванні центру обробки даних мережевий трафік можна охарактеризувати як північ-південь або схід-захід. Північ-південь описує трафік клієнт-сервер, який переміщується між центром обробки даних і місцем за межами мережі. Трафік з півночі на південь зазвичай зображується вертикально, щоб проілюструвати трафік, який надходить у центр обробки даних та з нього. На початку існування Інтернету більшість мережевого трафіку була з півночі на південь.

На відміну від цього, мережевий трафік схід-захід характеризує пакети даних, які переміщуються від сервера до сервера в центрі обробки даних. Термін схід-захід був натхненний мережевими діаграмами, які зображують трафік локальної мережі (LAN) по горизонталі. Апаратна віртуалізація та Інтернет речей (IoT) — це дві концепції, які стимулюють зростання мережевого трафіку зі сходу на захід.

Адміністратори можуть контролювати мережевий трафік за допомогою керування даними або визначення пріоритетів, а також можуть контролювати мережевий трафік, вимірюючи обсяг і типи трафіку. Мережевий трафік інкапсулюється в пакети, які є одиницями даних, які забезпечують навантаження в мережі. Наприклад, відвідавши веб-сторінку, користувач отримає серію пакетів. Типовий пакет буде містити до 1000-5000 байт.

Поширені проблеми мережевого трафіку включають збої компонентів, таких як збої сервера, маршрутизатора або брандмауера, або збої трафіку, наприклад вузькі місця та велика затримка. Вузькі місця можуть виникнути, коли не вистачає можливостей обробки даних для обробки поточного обсягу трафіку. Затримка, або затримка від введення в систему до її результату, може бути викликана тим, що компоненти в центрі обробки даних передають інформацію один одному, збільшуючи мережевий трафік. Висока затримка може виникати частіше з трафіком зі сходу на захід.

Щоб забезпечити якість мережі, адміністратори мережі повинні аналізувати, контролювати та захищати мережевий трафік. Моніторинг мережі дозволить контролювати комп’ютерну мережу на предмет збоїв і недоліків, щоб забезпечити безперервну роботу мережі. Інструменти, створені для сприяння моніторингу мережі, також зазвичай повідомляють користувачів про будь-які значні або неприємні зміни в продуктивності мережі. Моніторинг мережі дозволяє адміністраторам та IT-командам швидко реагувати на будь-які проблеми з мережею.

Щоб захистити мережевий трафік, можна використовувати інструменти безпеки мережі, такі як Nagios або Splunk. Інші методи, такі як увімкнення брандмауерів, також додадуть більше безпеки мережі. Для трафіку зі сходу на захід мікросегментація може зменшити поверхню атаки програми. Мікросегментація сегментує центр обробки даних на логічні

блоки, щоб дати можливість адміністраторам ЦОД налаштувати унікальні політики безпеки для кожного блоку.

1.3 Аналіз рівневої мережевої безпеки

Оскільки кіберзагрози постійно розвиваються у складності та масштабі, боротьба з ними передбачає розповсюдження захисту на всі системи в корпоративній мережі – сервери, бази даних, сервіси, встановлене програмне забезпечення тощо. Співробітники компанії розуміють і дотримуються принципів кібербезпеки, і не будуть (не)навмисно ставити під загрозу безпеку корпоративної мережі своїми діями [21-26].

Однак заходи кібербезпеки, що застосовуються всередині організації, можуть відрізнятися залежно від розміру компанії, її фінансових можливостей, галузі, в якій вона працює (регульована чи нерегульована), інформації, з якою вона має працювати під час господарської діяльності тощо.

Враховуючи ці та інші фактори, вдалося визначити три основні рівні захисту кібербезпеки. Залежно від їх складності, ці рівні можуть бути встановлені за допомогою IT-відділу компанії або постачальника послуг кібербезпеки.

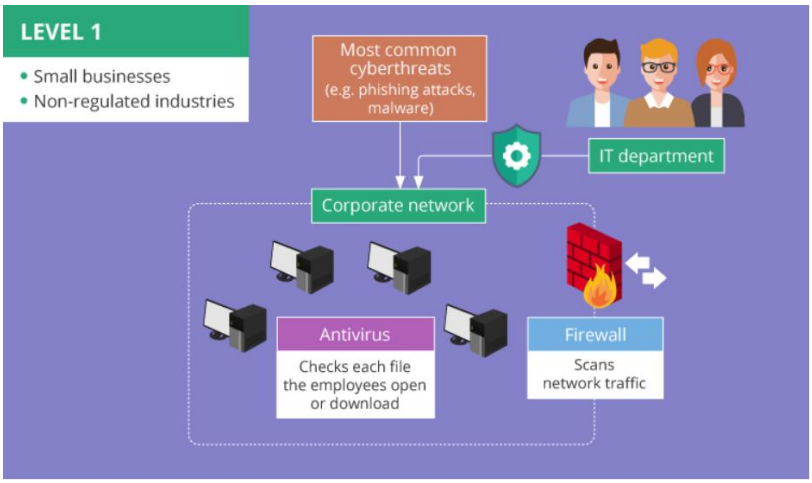

Рисунок 1.1 – Перший рівень кібербезпеки

Перший рівень забезпечує мінімальний захист, рисунок 1.1. Ключовим моментом кібербезпеки рівня 1 є забезпечення захисту корпоративної мережі від найпоширеніших кіберзагроз, наприклад, фішингових атак (посилання на шкідливі веб-сайти або завантаження, заражені вірусами, прикріплюються до електронних листів або миттєвих повідомлень і надсилаються співробітникам компанії). та зловмисне програмне забезпечення (зловмисне програмне забезпечення, яке потрапляє в мережу компанії через Інтернет або електронну пошту і існує у вигляді шпигунського програмного забезпечення, програм-вимагачів, зловмисників браузера тощо).

Мінімальний захист застосовується до малих підприємств, які працюють у нерегульованих галузях та мають суворо обмежені фінансові ресурси. Невеликі та маловідомі (принаймні, поки що) компанії, які не мають справу з інформацією, цінною для хакерів (наприклад, особистими даними клієнтів, такими як номери кредитних карток, паролі тощо), навряд чи можуть стати мішенню складних кібератак, таких як DDoS (відмова в обслуговуванні) або фішинг.

Мінімальним заходом кібербезпеки, необхідним для впровадження, є належним чином налаштований захист брандмауера, що працює разом із регулярно оновлюваним антивірусним програмним забезпеченням. Брандмауери сканують мережевий трафік, щоб виявити аномальні пакети або фрагменти пакетів. Антивіруси забезпечують захист від таких кіберзагроз, як програми-вимагачі, хробаки, шпигунські програми тощо, перевіряючи кожен файл, який співробітники відкривають або завантажують з Інтернету чи інших джерел.

Щоб застосувати ці заходи безпеки, немає потреби в організації окремого відділу кібербезпеки. IT-відділ компанії може взяти на себе відповідальність за це, оскільки впровадження захисту брандмауера, встановлення антивірусного програмного забезпечення та постійна

підтримка їхньої продуктивності не вимагає навичок, пов'язаних із кібербезпекою.

Проте рівень захисту корпоративної мережі слід регулярно перевіряти. Щорічне проведення оцінки вразливості та тестування на проникнення достатньо для невеликої організації, яка веде свій бізнес у нерегульованій галузі. Ці послуги кібербезпеки, що надаються на щорічній основі, не призведуть до великих витрат для компанії з обмеженим бюджетом. У той же час ці дії можуть допомогти системним адміністраторам бути в курсі слабких місць безпеки в мережі компанії.

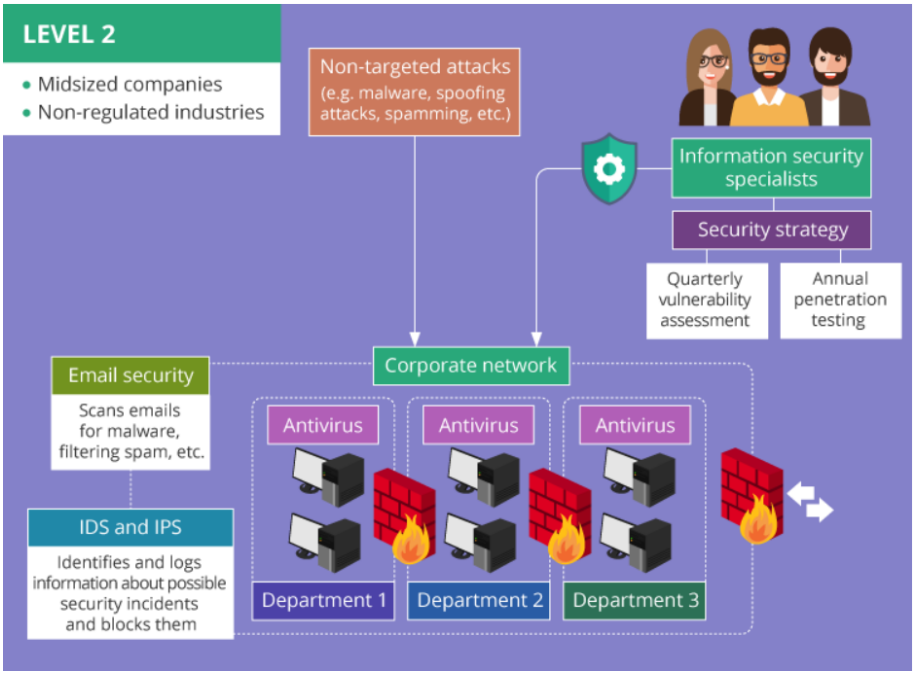

Рисунок 1.2 – Другий рівень кіберзахисту

Кібербезпека 2 рівня (рисунок 1.2) забезпечує захист корпоративної мережі від нецільових атак, наприклад, зловмисного програмного забезпечення, надісланого на низку адрес електронної пошти, підробних атак, розсилки спаму тощо. У цьому випадку мета зловмисників – вкрасти будь-яку цінну інформацію з будь-якої IP-адреси, схильної до відомих недоліків безпеки, які, можливо, існують у корпоративній мережі.

Імовірність того, що компанії середнього розміру стануть жертвами нецільових атак – велика. Оскільки, такі організації не мають потреби дотримуватись нормативних стандартів, вони, ймовірно, нехтують жорсткими заходами кібербезпеки у своїх мережах. Таким чином, з ними може бути легко піти на компроміс.

Для забезпечення розширеного захисту корпоративної мережі, окрім елементів мінімального захисту – брандмауерів та антивірусу – слід застосовувати такі компоненти:

– безпека електронної пошти, що передбачає використання різноманітних методів (сканування електронних листів на наявність шкідливих програм, фільтрація спаму тощо) для забезпечення безпеки корпоративної інформації як у “внутрішньому”, так і в “зовнішньому” повідомленні електронної пошти від будь-якої кібератаки, використовуючи електронну пошту як точку входу (шпигунське, рекламне програмне забезпечення, тощо);

– сегментація мережі, наприклад, сегментація мережі за відділами з сегментами, підключеними через брандмауери, які не дозволяють шкідливому коду чи іншим загрозам переміщатися з одного сегмента мережі в інший. Більше того, сегментація мережі передбачає відокремлення мережевих активів, у яких зберігаються дані компанії, від зовнішніх сегментів (веб-серверів, проксі-серверів), таким чином зменшуючи ризик втрати даних;

– система виявлення вторгнень (IDS) і запобігання вторгненням (IPS), що використовуються для ідентифікації та реєстрації інформації про можливі інциденти безпеки, блокування їх до того, як вони поширюються в мережевих середовищах тощо.

Для підтримки такого рівня мережевої безпеки компанії потрібні фахівці з інформаційної безпеки, відповідальні за виявлення та управління ризиками кібербезпеки, розробку процедур і політик безпеки тощо. Для цих

цілей компанія може створити власний відділ інформаційної безпеки або звернутися до керованої служби безпеки постачальник (managed security service provider (MSSP)).

Організація окремого відділу інформаційної безпеки передбачає великі витрати як на найм досвідченої служби безпеки, так і на придбання необхідного обладнання та програмного забезпечення. Робота з MSSP є більш економічно ефективним рішенням, яке дозволяє компанії зберігати фокус на основних бізнес-операціях. Тим не менш, для координації роботи з MSSP компанії все одно знадобиться співробітник служби безпеки.

Щоб контролювати ефективність захисту кібербезпеки, ретельно розроблена стратегія безпеки повинна передбачати щоквартальну оцінку вразливості та щорічне тестування на проникнення для виявлення, пом’якшення та управління ризиками кібербезпеки. Компанії потрібна стратегія кібербезпеки, оскільки вона зосереджена на захисті корпоративної мережі з урахуванням персоналу, який використовує свої персональні мобільні пристрої та ноутбуки в бізнес-цілях (BYOD), широкого використання хмарних обчислень тощо, а також надає прямі вказівки співробітникам компанії щодо прийнятної поведінки всередині корпоративної мережі.

Ключовим завданням кібербезпеки 3 рівня (рисунок 1.3) є забезпечення захисту корпоративної мережі від цілеспрямованих атак. Цей тип кібератак (фішинг, розповсюдження передових шкідливих програм, тощо) передбачає спеціально розроблені кампанії проти певної організації.

Жертвами цілеспрямованих атак зазвичай стають середні та великі підприємства, що працюють у регульованих галузях, наприклад, у банківській справі чи охороні здоров’я, чи державні установи. Це відбувається тому, що чим більша організація і чим більше даних вона має захищати (регульовані персональні дані, записи про медичне обслуговування

пацієнтів, інформація про банківські рахунки тощо), тим відчутнішими є результати успішних цілеспрямованих атак.

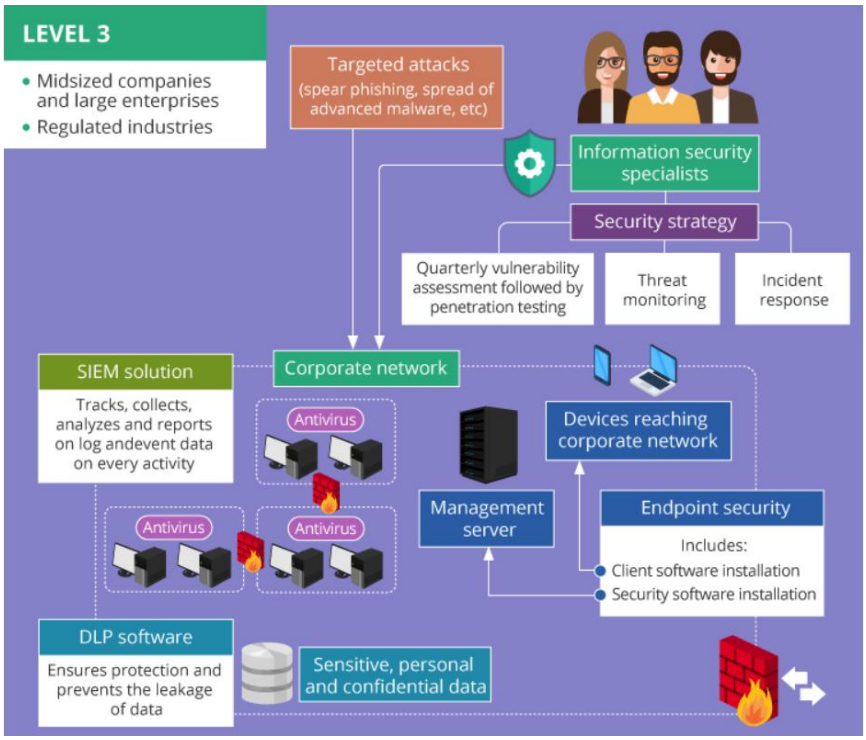

Рисунок 1.3 – Третій рівень кіберзахисту

Компанії, що працюють у регульованих сферах, повинні приділяти максимальну увагу підтримці захисту від кіберзагроз, дотримуючись правил і стандартів (HIPAA, PCI DSS тощо). Наступні компоненти кібербезпеки можуть допомогти закрити всі можливі вектори атак:

– безпека кінцевої точки. Цей метод безпеки передбачає захист доступу кожного пристрою (смартфона, ноутбука тощо), який досягає корпоративної мережі і таким чином стає потенційною точкою входу для загроз безпеці. Зазвичай захист кінцевої точки включає встановлення спеціального програмного забезпечення безпеки на сервері керування в корпоративній мережі разом із встановленням клієнтського програмного забезпечення на кожному пристрої. Поєднання цих заходів дає змогу відстежувати дії користувачів під час віддаленого доступу до корпоративної мережі зі своїх смартфонів, планшетів та інших пристроїв. Таким чином,

компанія отримує кращу видимість у режимі реального часу щодо всього спектру потенційних загроз безпеці, з якими вони можуть мати справу;

– запобігання втраті даних (Data loss prevention (DLP)). Застосування цього заходу надзвичайно важливо на підприємстві, що займається фінансовою або медичною сферою. Програмне забезпечення DLP забезпечує захист та запобігає витоку конфіденційних, особистих та конфіденційних даних, наприклад, номерів кредитних карток клієнтів, номерів соціального страхування тощо, надаючи адміністраторам DLP повний контроль над типами даних, які можуть передаватися за межі корпоративної мережі. DLP може відхиляти спроби пересилати будь-яку ділову електронну пошту за межами корпоративного домену, завантажувати корпоративні файли в хмарні сховища з відкритим кодом тощо;

– управління інформацією та подіями безпеки (Security information and event management (SIEM)). Рішення SIEM відстежують, збирають, аналізують і звітують про дані журналів і подій про кожну діяльність, що відбувається в IT-середовищі, що дозволяє уникнути ситуацій “я не знаю, що сталося” у разі злому мережі компанії. Серед переваг SIEM – централізація зібраних даних журналу, забезпечення підтримки для виконання вимог PCI DSS, HIPAA та інших нормативних актів, що забезпечує реагування на інциденти в режимі реального часу.

Для належної роботи із зазначеними рішеннями безпеки найкращим буде поєднання зусиль окремого відділу інформаційної безпеки та допомоги MSSP. Для багатьох компаній надання MSSP повного доступу та контролю над конфіденційними даними, персональною інформацією клієнтів тощо виглядає досить ризиковано, особливо з точки зору відповідності вимогам безпеки. Однак підписати детальну угоду про рівень обслуговування з компанією, що надає послуги з кібербезпеки, і делегувати частину обов’язків із кіберзахисту зовнішньому MSSP має сенс. Це дозволяє підприємствам

отримувати цілодобовий моніторинг стану безпеки та звітність та одночасно знизити витрати на захист кібербезпеки.

Серед необхідних заходів кібербезпеки – розробка та підтримка стратегії безпеки, проведення оцінки вразливості з подальшим тестуванням на проникнення щоквартально (краще проводити перед кожною аудиторською перевіркою, щоб відповідати стандартам і нормам), забезпечення постійного моніторингу загроз та організація структурованого реагування на інцидент (incident response (IR)).

Моніторинг загроз передбачає постійний моніторинг корпоративної мережі та кінцевих точок (серверів, бездротових пристроїв, мобільних пристроїв тощо) на наявність ознак загроз кібербезпеці, наприклад, вторгнення або спроби вилучення даних. На сьогоднішній день моніторинг загроз набуває ще більшого значення з тенденцією на підприємствах наймати працівників дистанційно та застосовувати політику BYOD, що ставить під додатковий ризик захист корпоративних даних та конфіденційної інформації.

Реагування на інциденти (IR) стосується ситуацій, коли порушення безпеки вже мали місце. Таким чином, компанії потрібна спеціальна внутрішня або стороння команда, підготовлена до інцидентів, готова виявляти реальні події, знаходити причини та реагувати на загрози кібербезпеці з мінімальним збитком і мінімальним часом, необхідним для відновлення після атаки. ІК-діяльність запобігає переростанню дрібних проблем у більші, наприклад, порушення даних або відключення системи.

Компанії повинні приділяти особливу увагу захисту своїх хмарних активів. Нині зберігання критично важливих для бізнесу даних у хмарі стає звичайною практикою. Вибір хмарних обчислень має сенс, оскільки це дозволяє підприємствам заощадити витрати та підвищити ефективність бізнес-операцій, які вони здійснюють.

Однак хмарні середовища представляють відносно нові області для команд безпеки, яким необхідно організувати та підтримувати заходи

кібербезпеки всередині корпоративної мережі. Це також призводить до нових проблем безпеки, оскільки “хмарна природа” означає відсутність контролю для системних адміністраторів над ресурсами, які використовує компанія, і даними, які вони зберігають у хмарі.

Фахівці з кібербезпеки застосовують різні стратегії для захисту хмарних ресурсів залежно від хмарної моделі. До найбільш розповсюджених відносяться інфраструктура як послуга (IaaS) і платформа як послуга (PaaS)

В обох випадках стратегія кібербезпеки схожа на підхід до захисту локальної корпоративної мережі. Різниця полягає в “факторі віддаленості”. Основним завданням компанії є вибір надійного постачальника IaaS/PaaS, розміщення серверів у хмарі, яку вони пропонують, і встановлення відповідного рівня контролю над наданими віртуальними машинами. Існують найкращі методи, які можна застосувати для забезпечення безпеки IaaS/PaaS, наприклад, забезпечення належного шифрування даних, що зберігаються та надсилаються в сторонню хмару, моніторинг мережевого трафіку на наявність шкідливих дій, регулярне резервне копіювання даних тощо.

Деякі постачальники рішень IaaS або PaaS також надають своїм клієнтам “вбудовані” послуги кібербезпеки, але це не звичайна практика. Наприклад, Microsoft Azure пропонує клієнтам різноманітні способи захисту робочих навантажень у хмарі, захисту програм від поширених уразливостей тощо. Amazon Web Services (AWS) представляє іншого постачальника хмарних послуг, який надає своїм клієнтам застосовувані хмарні заходи безпеки (вбудовані у брандмауерах, можливостях шифрування тощо), послуги оцінки безпеки для виявлення слабких місць кібербезпеки, керування ідентифікацією та доступом для визначення доступу користувачів до ресурсів AWS тощо.

Програмне забезпечення як послуга (SaaS) означає, що у цьому випадку постачальник SaaS бере на себе відповідальність за створення,

розміщення та захист програмного забезпечення, яке вони пропонують. Однак компанії ще потрібно попрацювати, щоб забезпечити безпеку рішення. Їм необхідно зосередитися на управлінні доступом до програм для своїх співробітників з урахуванням відділів, в яких вони працюють, займаних посад тощо. Таким чином, першочерговим завданням силовиків компанії є встановлення контролю доступу користувачів, тобто налаштування параметрів правильно.

Office 365 являє собою приклад хмарного рішення з багаторівневою безпекою. Вбудовані в нього функції кібербезпеки дозволяють постійно контролювати центри обробки даних, виявляти та запобігати зловмисним спробам доступу до особистої чи конфіденційної інформації, шифрувати збережені та передані дані, використовувати антивірусний захист і захист від спаму, щоб захиститися від загроз кібербезпеці, що надходять у корпоративну мережу ззовні, тощо

1.4 Висновки до першого розділу

Перший розділ кваліфікаційної роботи висвітлює організацію розробки та будови мережі через впровадження точок входу в мережу з подальшим їх контролем та захистом, що дає змогу використовувати збільшений контроль у порівнянні з традиційними підходами. Проведено аналіз типів мережевих потоків даних для визначення нормального виду мережі, що уможливлює створення систем моніторингу за нетиповою роботою профілю мережевих ресурсів. Здійснено аналіз рівневого кіберзахисту, що показало можливість організації захисту даних на основі рівнів де кожен має свої вимоги до персоналу, наборів обладнання та вимог відповідності стандартам.

2 МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ ЗОНОВОЇ БЕЗПЕКИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

2.1 Індикатори компроментування комп'ютерної мережі

З огляду на ескалацію порушень безпеки через пандемію, постачальники послуг кібербезпеки та співробітники служби безпеки зосереджують свої зусилля на ранньому виявленні кіберзагроз. Щоб якомога швидше отримати ознаки незахищеності мережі, спеціалісти з інформаційної безпеки (ІБ) використовують індикатори компромісу (indicators of compromise (IoCs)) [27-35].

Індикатори компромісу вказують на потенційно шкідливі дії в системі чи мережі та артефакти, які з високою впевненістю вказують на комп'ютерне вторгнення.

Прикладами підозрілої діяльності можуть служити незвичайні моделі трафіку між внутрішніми системами, незвичайні моделі використання привілейованих облікових записів, адміністративний доступ до вашої мережі з непередбачуваного географічного розташування. Цифрові артефакти включають підозрілі IP-адреси та імена хостів, URL-адреси та доменні імена бот-мереж, хеші MD5 файлів шкідливих програм, сигнатури вірусів, записи реєстру Windows, мережеві процеси та служби.

Адміністратори безпеки знаходять ознаки компроментування в журналах хоста, а також у журналах мережевих пристроїв. Ідентифіковані IoC застосовуються для виявлення майбутніх атак за допомогою автоматизованих рішень безпеки (системи SIEM, антивіруси, IDS/IPS, HIDS/HIPS).

Є два джерела IoC: зовнішнє і внутрішнє. Зовнішні репозиторії IoC включають комерційні джерела, а також безкоштовні. Різні постачальники консультацій з інформаційної безпеки (RSA, Norse, McAfee, Symantec) та

дослідницькі групи з безпеки (IBM X-Force) надають своїм клієнтам IoC на комерційній основі. Крім того, дані IoC поширюються кількома групами Центру обміну інформацією та аналізу (Sharing and Analysis Center (ISAC)) у кількох галузях. Наприклад, FS ISAC (фінанси), R-ISAC (роздрібна торгівля), IT-ISAC (IT).

Безкоштовні джерела IoC можна знайти на спеціальних сайтах, наприклад, IoC bucket. Цей веб-сайт дозволяє завантажувати та отримувати додаткову інформацію про різні індикатори компромісу, а також заохочує завантажувати нові IoC та ділитися ними з IT-спільнотою.

Ще одним чудовим джерелом даних IoC є Google. Фахівці з безпеки використовують службу Google Alerts або навіть простий пошук Google для отримання відповідних результатів.

Основним недоліком зовнішніх індикаторів компроментування є те, що вони можуть генерувати хибнопозитивні результати при застосуванні до певного середовища. Тому спеціалісти з корпоративної інформаційної безпеки беруть на себе роль детективів і розробляють спеціальні IoC для своїх мереж і хостів.

Авторка Dark Reading Еріка Чіковскі описує у своїй статті 15 ключових показників компроментування:

– незвичайний вихідний мережевий трафік;

– аномалії в діяльності облікового запису привілейованого користувача.

– географічні порушення.

– червоні прапорці входу;

– збільшення обсягу читання бази даних;

– розміри відповідей HTML;

– велика кількість запитів на той самий файл;

– невідповідний трафік порту-програми;

– підозрілі зміни реєстру або системних файлів;

– незвичайні запити DNS;
– несподіване виправлення систем;
– зміни профілю мобільного пристрою;
– патчі даних у неправильному місці;
– веб-трафік з нелюдською поведінкою;
– ознаки активності DDoS.

Цей список не є вичерпним. Зазвичай фахівці з інформаційної безпеки створюють нові IoC на основі інформації з конференцій, додаткової інформації про нещодавно виявлені вразливості та попередні інциденти.

Дані IoC дозволяють фахівцям з інформаційної безпеки визначити, що мережа вже зламана, і отримати подробиці про те, що сталося, хто був залучений і коли сталася атака.

Консультанти з інформаційної безпеки інтегрують індикатори компроментування в автоматизовані рішення безпеки (наприклад, системи SIEM, IDS/IPS, HIDS/HIPS, антивіруси), забезпечуючи додаткові докази того, чи є даний елемент шкідливим. Зібравши та впровадивши індикатори компромату для певної загрози, спеціалісти з безпеки можуть сканувати мережу в пошуках будь-якої з них. Наявність файлів з певним хешем або запущеними процесами під певним іменем є ознакою того, що мережа була зламана.

Індикатори компроментування діють як червоні прапорці, які сигналізують спеціалістам із інформаційної безпеки про потенційну або триваючу кібератаку. Зокрема, вони корисні для пошуку APT (advanced persistent threats). Атака APT зазвичай обходить традиційні технології безпеки, оскільки її сигнали дуже слабкі. Перш ніж виявити, APT може тривати протягом року в латентній формі. IoC дозволяють спеціалістам із інформаційної безпеки виявляти присутність APT та зупиняти вилучення даних. Ось кілька прикладів поширених IoC для виявлення Carbanak (кампанія в стилі APT, яка в основному націлена на фінансові установи):

– підключення до командно-контрольних серверів, розташованих у підозрілому місці (зокрема, в Китаї);

– успішне виконання нового віддаленого коду в мережі, що призводить до встановлення Carbanak в системі жертви;

– запис у шлях до файлу через конфіденційні системні каталоги, такі як System 32. Carbanak, наприклад, копіює себе в “%system32%com” з іменем “svchost.exe” із системою атрибутів файлу, прихованою та доступною лише для читання;

– поява нових сервісів або автозапусків. Наприклад, Carbanak створює нову службу, щоб забезпечити їй привілеї автозапуску;

– наявність інструментів віддаленого адміністратора (PAT). Зловмисники Carbanak використовують Ammyy Admin RAT, оскільки він зазвичай використовується адміністраторами, і тому він знаходиться в білому списку;

– наявність віддаленого входу. У разі атаки Carbanak, журнали інструментів RAT свідчать про те, що доступ до них був здійснений з двох різних IP-адрес, які використовували зловмисники та розташовані в Україні та Франції;

– наявність незвичайних IT-інструментів. Зловмисники Carbanack використовують додаткові інструменти, такі як Metasploit, PsExec, Mimikatz, щоб отримати контроль над мережею жертви.

IoC покращують позицію безпеки компанії, зосереджуючи увагу на криміналістичному аналізі компромату, який уже відбувся. Це скоріше реактивний, ніж проактивний підхід. Такі індикатори допомагають запобігти повторюваним і постійним загрозам, але вони не призначені для виявлення нових або модифікованих загроз, наприклад, атак без шкідливого програмного забезпечення або експлойтів нульового дня.

Однак більшість атак, включаючи APT, використовують сценарії, які хтось уже використовував у подібних випадках порушення безпеки. Саме

тому IT-спільнота документує та активно ділиться індикаторами компромату для реагування на інциденти та покращення комп'ютерної криміналістичної експертизи.

2.2 Глибоке тестування мережі для знаходження вразливостей

Компанії проводять тестування на проникнення, щоб знайти діри у своїй корпоративній мережі, перш ніж хакери скористаються ними. На додаток до надійної оцінки безпеки мережі, це може допомогти CISO (Chief Information Security Officer) перевірити, чи готова команда безпеки компанії боротися з порушеннями безпеки мережі [36-40].

Тестування на проникнення може бути оголошеним або неоголошеним. Щоб зрозуміти, чи готовий відділ безпеки до дій, CISO варто розглянути можливість неоголошеного тестування. Інакше процес буде нагадувати скоріше виставковий виступ, ніж щоденну гарантію безпеки.

CISO отримає уявлення про загальну кваліфікацію відділу безпеки зі звіту про тестування на проникнення, точніше, про описані в ньому вразливості. Враховуючи той факт, що жодна мережа не вільна від вразливостей, все ще існує кілька легковикористаних вразливостей, яких добре керована мережа не повинна мати. Наявність таких вразливостей у звіті про тестування на проникнення говорить про те, що фахівці з безпеки компанії не володіють достатнім рівнем знань для забезпечення гідного рівня безпеки корпоративної мережі. Це означає, що компанія не тільки наражається на найтривіальніші кіберзагрози, але й втрачає додаткові гроші на додаткову роботу тестера на проникнення.

Крім того, розглядаються тривіальні вразливості, які не пропустять пильні спеціалісти з безпеки. Отже, якщо звіт про тестування на проникнення містить ці проби в безпеці, це означає, що рівень компетенції співробітників служби безпеки є дуже сумнівним.

Своєчасні виправлення ОС безпеки покривають величезну кількість серйозних вразливостей безпеки, які можуть легко використати зловмисники. Наведемо як приклад горезвісну атаку WannaCry. У травні 2017 року це програмне забезпечення-вимагач спричинило хаос у сотнях тисяч комп'ютерів у 150 країнах. Атака була спрямована на уразливості Microsoft Windows, які могли бути закриті оновленим виправленням.

Хоча багато організацій постійно оновлюють свої операційні системи, програми часто залишаються осторонь безпеки. Однак уразливості додатків можуть бути не менш руйнівними. Наприклад, атака SQL Slammer 2003 року, коли дуже заразний комп'ютерний хробак викликав відмову в обслуговуванні деяких інтернет-хостів і за кілька хвилин заразив 75 000 жертв. Хробак використав помилку переповнення буфера в програмному забезпеченні баз даних Microsoft SQL Server і Desktop Engine. Патч для усунення уразливості Microsoft був випущений шість місяців тому, але більшість організацій проігнорували його.

Усі програми від корпоративних баз даних до настільних програм вимагають відповідного виправлення. Така практика не тільки гарантує відсутність уразливостей, пов'язаних із додатками, але й робить тестування на проникнення більш ефективним, надаючи більше часу на виявлення складних недоліків безпеки, заощаджуючи таким чином додаткові гроші компанії.

Оскільки доступна велика кількість виправлень для ОС і програм, адміністраторам безпеки може бути важко не відставати від останніх виправлень. У цьому випадку CISO повинні переконатися, що їхні групи безпеки використовують автоматизовані інструменти оновлення, наприклад, FileHippo Update Checker, Update Notifier або Windows Server Update Services (WSUS). Сумлінний спеціаліст із безпеки не лише встановлює інструмент оновлення та перекладає на нього кошти, а й регулярно перевіряє наявність останніх виправлень. Крім того, він чи вона забезпечить успішне

встановлення виправлень, перевіряючи, чи застосовано виправлення відповідно до реєстру, чи потрібне перезавантаження для завершення інсталяції, чи є правильні версії файлів .dll та .exe.

Часто тестування на проникнення виявляє вразливі місця в мережевих службах, які були пропущені та залишені увімкненими, навіть якщо вони не використовуються та не виправлені. Наприклад, невиправлені вразливості в таких службах управління, як System Management від Hewlett Packard і OpenManage від Dell Inc., часто служать точками доступу до корпоративної мережі.

Подібну загрозу становлять невикористані мережеві протоколи. Відповідальні фахівці з безпеки обов'язково вимикають протоколи віддаленого керування, такі як telnet або протокол віддаленого робочого столу (RDP), коли вони не використовуються. Те ж саме з NetBIOS і роздільною здатністю локальної багатоадресної передачі (LLMNR). Ці два старі протоколи трансляції, які використовуються серверами Windows XP і Windows 2003 для зворотної сумісності. Якщо залишити ці застарілі інструменти Microsoft без нагляду, це збільшує поверхню атаки.

Забезпечення надійності пароля має здаватися очевидним для спеціалістів із інформаційної безпеки. Проте звіти про тестування на проникнення постійно виявляють уразливості, пов'язані з паролем. Наведемо найпоширеніші проблеми:

– використання стандартних і слабких паролів. Наприклад, старі версії Microsoft SQL Server створюють обліковий запис адміністратора з паролем "password".

– використання слабких паролів (довжиною менше 7-8 символів, без спеціальних символів або цифр).

– зберігання файлів SAM (Sequence Alignment Map) у добре відомому місці. Наприклад, щоб зламати паролі Windows, хакер повинен отримати хеші, що зберігаються у файлі Windows SAM, який зазвичай

знаходиться в кількох широко відомих місцях (C:\WINDOWS\repair або C:\Windows\System32\config). Ці файли заслуговують на більш невідоме розташування, оскільки вони містять ключову інформацію безпеки.

Те, як спеціалісти з безпеки ставляться до політики паролів, показує, наскільки вони професійні. Усі облікові записи керування мають бути налаштовані на регулярне скидання надійних паролів.

Адміністратори безпеки можуть забути обмежити доступ до таких поширених мережевих цілей, як веб-інтерфейси, логіни для відеоконференцій, бекдори додатків, послуги FTP, приватні API, інтерфейси віддаленого керування, telnet і SSH. Це дає тестеру проникнення, а отже, і зловмиснику різноманітні точки доступу до мережі, щоб скомпрометувати і ставить під сумнів професіоналізм співробітників служби безпеки.

2.3 Мережеві архітектури захисту інформаційних ресурсів

Архітектура безпеки є основою захисту будь-якої організації від кіберзломів. Ці методи безпеки, послуги та технології призначені для захисту IT-інфраструктури та пристроїв організації, водночас забезпечуючи безперебійне функціонування бізнесу [41-45].

Універсальний підхід до кібербезпеки практично неможливий, оскільки різні підприємства мають різноманітні та унікальні вимоги. Архітектори безпеки консультуються з підприємствами, щоб зрозуміти, як вони працюють, їхню цільову аудиторію, послуги та обробку даних. Архітектори також розглядають, як компанія взаємодіє з клієнтами цілісно, щоб знайти відповідне рішення безпеки.

Ідеальна архітектура безпеки повинна бути достатньо гнучкою, щоб адаптуватися та забезпечувати безпеку для бізнесу, незважаючи на безперервний розвиток домену кіберзагроз.

Універсальні мережі безпеки мають важливе значення, оскільки організації розширюють послуги далеко за традиційні рамки та беруть участь у кампаніях цифрового розширення. Віртуальні порушення обійшлися організаціям у майже 3 мільйони фунтів стерлінгів, як повідомляє IBM. Ці приголомшливі цифри підкреслюють потребу компаній посилити контроль над хмарами та захистити свої активи від цифрового компромісу.

В останні роки багато технологій архітектури безпеки стали віддавати перевагу моделі “нульової довіри”. Ця сувора модель безпеки, також відома як безпека без периметра, вимагає перевірки кожного запиту, незалежно від того, чи знаходяться системи всередині або поза периметром. Ідеологія цього фреймворка діє, оскільки дослідження показують, що багато атак здійснювалися всередині мережі. Використання контролю доступу та встановлення кількох контрольних точок у мережі обмежить ризик проникнення шкідливих програм.

Незважаючи на те, що підприємства можуть самостійно створювати прості системи безпеки мережі, багато з них не володіють необхідними технологіями для ефективного управління ризиками кібербезпеки. Понад 50% організацій у Великобританії передають свої потреби в безпеку експертам. Оскільки це фундаментальний крок при створенні нових або впровадженні вдосконалених архітектур, підприємства повинні звертатися за допомогою до відповідних організацій для забезпечення захищених проектів та дослідження мереж.

Щоб визначити, чи важко зламати мережу, архітектори безпеки повинні знати, як загрози атакують потенційну ціль. Для цього архітектори повинні добре розуміти процеси та бізнес-цілі своєї організації. Вони повинні розуміти, як виникають вразливості та як учасники загроз використовують їх.

Якщо система легко схильна до кібератак, можливо, її потрібно буде перепроектувати, реструктурувати або налаштувати по-іншому, щоб зменшити ризик злому даних.

Тим не менш, ми можемо встановити деякі загальні вимоги до ефективної архітектури безпеки. Вони складаються з трьох основних компонентів:

– люди – вони встановлюють цілі безпеки та визначають рушії бізнесу;

– процеси – вони визначають методи та принципи безпеки, які найкраще підходять для бізнесу на основі оцінки потреб;

– інструменти – архітектурна структура, розроблена для задоволення бізнес-цілей і завдань.

Закріплені в політиці компанії, ці компоненти повинні захищати активи організації від кіберзагроз. Таким чином, архітектури безпеки допомагають керівництву забезпечити послідовність прийняття рішень у всій IT-сфері. Архітектура має бути стратегічно розроблена та реалізована таким чином, щоб підтримувати цілі бізнесу.

Розробка технологій мережевої безпеки не є одноразовим процесом. Оскільки підприємства ростуть і розширюються, а технології розвиваються, середовище, що постійно змінюється, вимагає постійного моніторингу та модифікації архітектури безпеки. Найкращі методи системи безпеки компанії слід періодично тестувати та перевіряти, щоб переконатися, що вона продовжує відповідати потребам бізнесу.

Апаратні та програмні ресурси, які архітектори використовують для розгортання, запуску та моніторингу безпеки мережі, слід регулярно перевіряти та налаштовувати для підтвердження оптимальної продуктивності.

У індустрії технологій часто доступні нові рішення для вирішення проблем безпеки. Коли в архітектурі безпеки відбувається зміна технології, архітектор безпеки повинен визначити, чи потрібно вносити зміни відповідно до найкращих практик.

На рисунку 2.1 показано логічну архітектуру захисту мережі запропоновану компанією Gartner.

Тут пропонуються основні поняття для розуміння сучасної архітектури мережевої безпеки. Починаючи з ролей та обов'язків керівників мережевої безпеки, а потім логічної архітектури, відображення діапазону вимог безпеки, що створює міцну основу, на якій можна будувати захищені мережі.

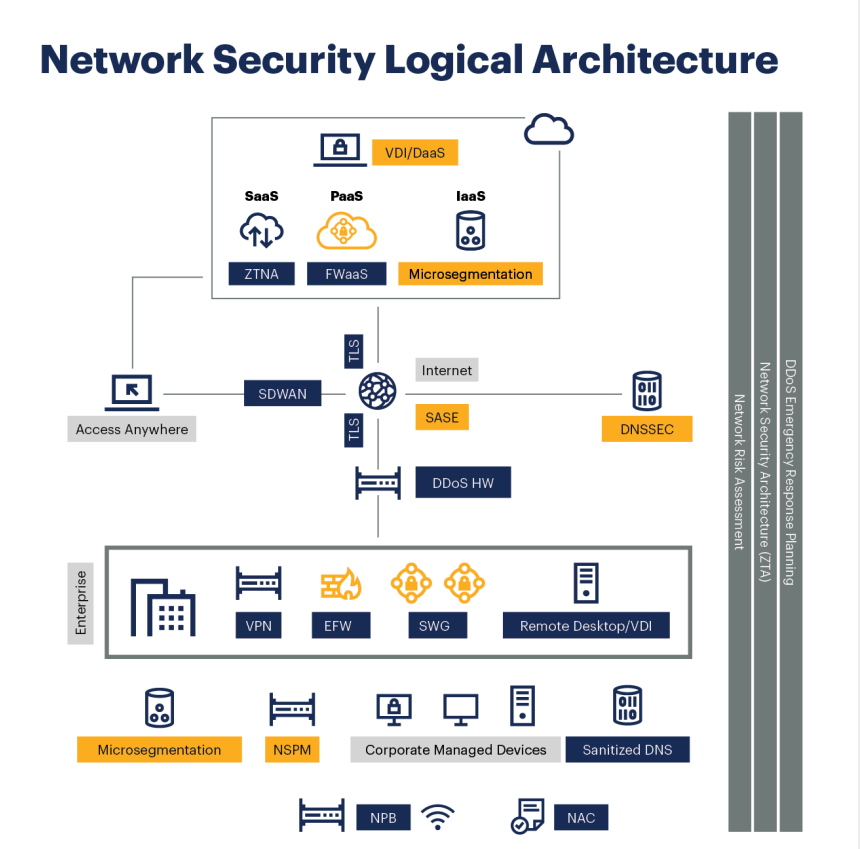

Рисунок 2.1 – Логічна архітектура захисту мережі

Існують і інші фреймворки, що дають змогу опираючись на них будувати захищені мережеві рішення.

SABAS розшифровується як Sherwood Applied Business Security Architecture. Це основа для розробки архітектури кібербезпеки, орієнтованої на ризики. Ця орієнтована на політику структура передбачає відповіді на основні питання безпеки та забезпечення інформації: хто, що, коли і чому.

Він гарантує, що безпека вбудована в IT-архітектуру підприємства або процеси управління IT, але не включає технічні реалізації.

Міжнародний стандарт ISO 27001 встановлює специфікації для управління системами управління інформаційною безпекою (СУІБ). Структура дотримується підходу, що ґрунтується на оцінці ризику, який вимагає від корпоративних органів вжити заходів для виявлення загроз безпеки, які впливають на їхні інформаційні системи.

Стандарт пропонує набір із 114 найкращих методів контролю безпеки, які професіонали можуть застосовувати на основі ризиків, з якими стикаються підприємства. Вони впроваджуються як частина організаційної структури всієї компанії для досягнення сертифікованої відповідності.

TOGAF розшифровується як The Open Group Architecture Framework, яка допомагає визначити та впровадити методи вирішення бізнес-проблем. Він зосереджений на основах архітектури безпеки, спрямований на досягнення заданого обсягу та мети вирішення проблеми. Тут варто звернути увагу на те, що він не вирішує конкретні проблеми безпеки.

Мінімальний стандарт кібербезпеки (Minimum Cyber Security Standard (MCSS)) є частиною серії технічних стандартів, розроблених урядом Великобританії у співпраці з NCSC.

Він визначає низку обов’язкових кіберстандартів, яких усі урядові відомства повинні досягти, щоб виконати свої зобов’язання згідно з SPF та Національною стратегією кібербезпеки.

Інші організації та підприємства також можуть використовувати MCSS у Великобританії, щоб створити основу для своїх заходів безпеки. Інтегрована видимість і каталогізація цифрових активів, контроль безпеки веб- та мобільних додатків є незамінними частинами процесу відповідності MCSS.

Структура кібербезпеки NIST була розроблена в першу чергу для урядових установ і компаній США. Його головною метою було зміцнення

критичної інфраструктури агентств. Незалежно від того, для чого регуляторні органи США створили структуру, вона виявилася ефективною, допомагаючи організаціям захистити себе від зовнішніх і внутрішніх атак. Структура також застосовна до компаній із Великобританії. Багато компаній продовжують інтегрувати його у свої системи безпеки.

Компанія Cisco пропонує свій погляд на організацію зонової безпеки для мереж. На рисунку 2.2 показано загальну архітектуру захищеної мережі.

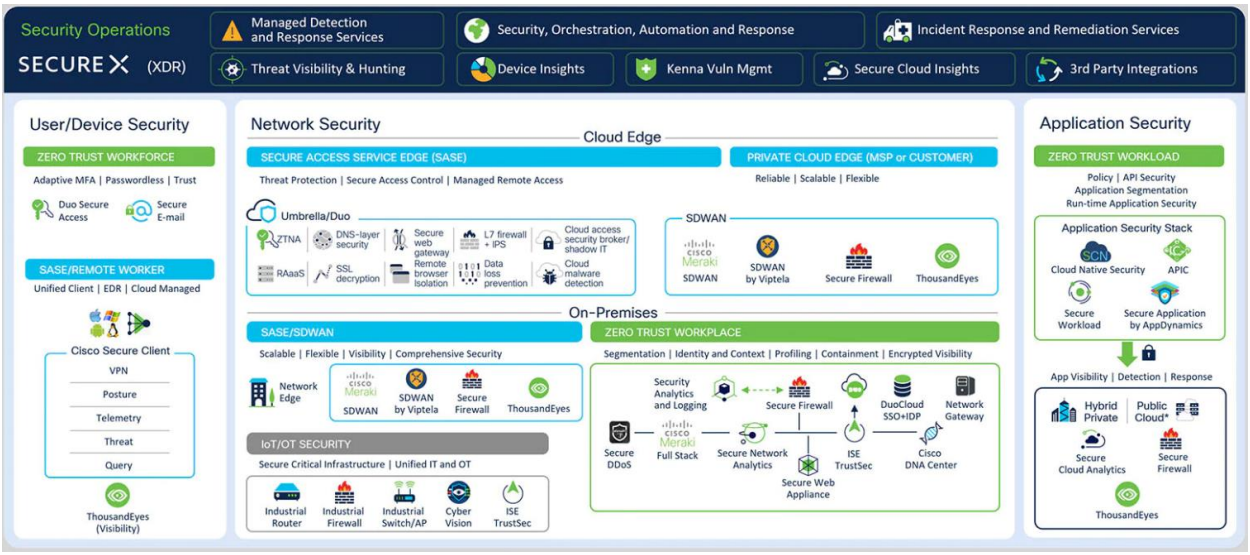

Рисунок 2.2 – Загальна архітектура захисту мережі від Cisco

Огляд включає кілька поширених випадків використання. Одним із них, що охоплює всю архітектуру, є рішення Cisco Zero Trust (зелені горизонтальні смуги) для робочої сили, робочого місця та робочого навантаження. Іншим є рішення Cisco SASE (сині горизонтальні смуги), яке складається з продуктів категорій безпеки користувача/пристрою та мережі. Cisco Umbrella, основний компонент SASE в області хмари, служить центром безпечного з'єднання для всіх віддалених користувачів і меж/філій мережі. Cloud edge також включає приватну межу хмари (коротша синя горизонтальна смуга), яка дозволяє деяким клієнтам вибірково створювати власний край SASE за допомогою засобів спільного розміщення, таких як Equinix, Megaport та інші. Операції безпеки (темно-синій горизонтальний

рядок SecureX) контролюють усі модулі під ним. Він отримує телеметрію для моніторингу, розслідування та аналізу (з розвідкою про загрози Talos) і надає відповіді за допомогою оркестровки.

На рисунку 2.3 показано вигляд загальної ідентифікації за допомогою архітектури запропонованої компанією Cisco.

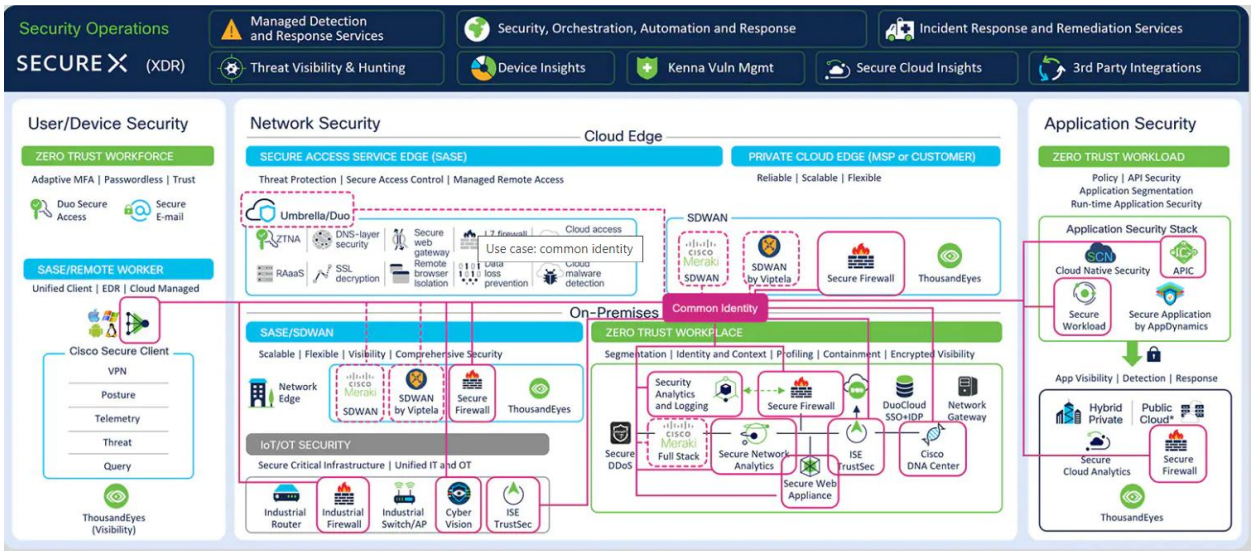

Рисунок 2.3 – Загальна ідентифікація

Cisco pxGrid полегшує спільний доступ до контексту користувача/пристрою по всій мережі та в компоненті безпеки додатків з нульовою довірою для робочих навантажень для гібридних приватних/публічних хмар, таких як AWS, Azure і GCP. Спільний доступ до ідентифікаційної інформації за допомогою Umbrella в межах хмари доступний сьогодні за допомогою з’єднувачів AD/LDAP для розширення локальної ідентифікації на хмару Umbrella як частину контролю політики Umbrella. Розширення ідентифікації в Umbrella за допомогою pxGrid стане можливістю в майбутньому і дозволить клієнтам Umbrella збагатити свої політики доступу до хмари за допомогою більш детальної інформації про контекст. Багато клієнтів зі списку Fortune 1000 використовують pxGrid і використовують його для інтеграції будь-яких сторонніх екосистемних рішень pxGrid у свої системи ідентифікації та доступу.

На рисунку 2.4 показано узгоджену політику безпеки у хмарних середовищах.

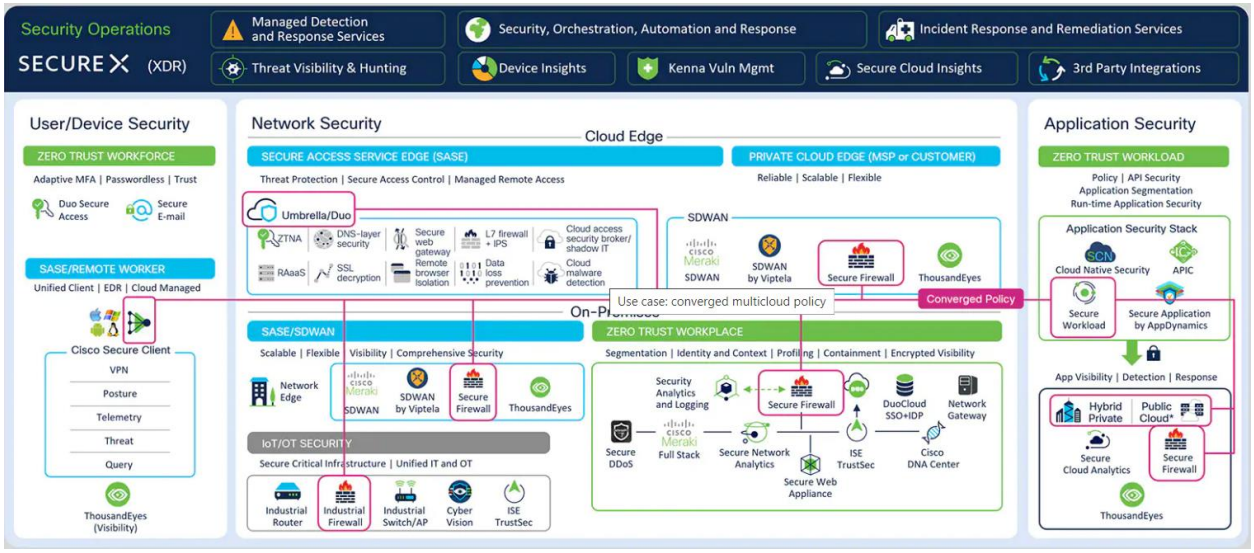

Рисунок 2.4 – Узгоджена політика безпеки у хмарах

Конвергентну мультихмарну політику можна створювати й керувати поетапно, починаючи з робочого навантаження додатків і переходячи до кінцевих точок. Багато клієнтів просять синхронізувати політику робочого навантаження та периметра центру обробки даних, щоб покращити керування політикою брандмауера в цілому. Наприклад, всеосяжну політику безпечного робочого навантаження можна синхронізувати з політиками AWS VPC Network Security Group, в яких працюють агенти EC2 і безсерверні програми. Крім периметра центру обробки даних, механізм політики робочого навантаження може синхронізуватися з мережевими брандмауерами для підвищення ефективності роботи. Це вимагає подальшого вивчення та планування мережевих політик через складність об’єднання кількох шарів брандмауерів. Ця концепція багатохмарного конвергентного механізму політики знаходиться на стадії розробки і буде продовжувати розвиватися та вдосконалюватися на основі типових випадків використання клієнтів.

На рисунку 2.5 показано інтеграцію Secure access service edge (SASE).

Рішення Cisco SASE через Cisco Umbrella забезпечує захист від загроз і безпечний доступ, де б користувач не знаходився – вдома, у місцевій кав'ярні, в штаб-квартирі чи регіональному офісі. Комбінація з SD-WAN забезпечує застосування відповідної політики доступу, при цьому користувачеві не потрібно вирішувати, як безпечно підключитися. Функція автотунелювання рішення Cisco SASE – з використанням, наприклад, Viptela vManage – дозволяє клієнтам легко створювати тисячі безпечних IP-тунелів за допомогою кількох кліків і введення ключів API. Використовуючи можливості безпечного інтернет-шлюзу (Secure Internet Gateway (SIG)) Umbrella, клієнти можуть користуватися такими функціями безпеки, як безпека DNS, Snort IPS, брандмауер із хмарою, віддалена ізоляція браузера, CASB, перевірка шкідливого програмного забезпечення тощо. Ці розширені функції безпеки та розгортання зменшують людські помилки під час великомасштабних розгортань і допомагають увімкнути політики, що містять багато контексту, які пом'якшують несанкціонований доступ.

На рисунку 2.5 показано реалізацію Zero Trust Network Access (ZTNA)

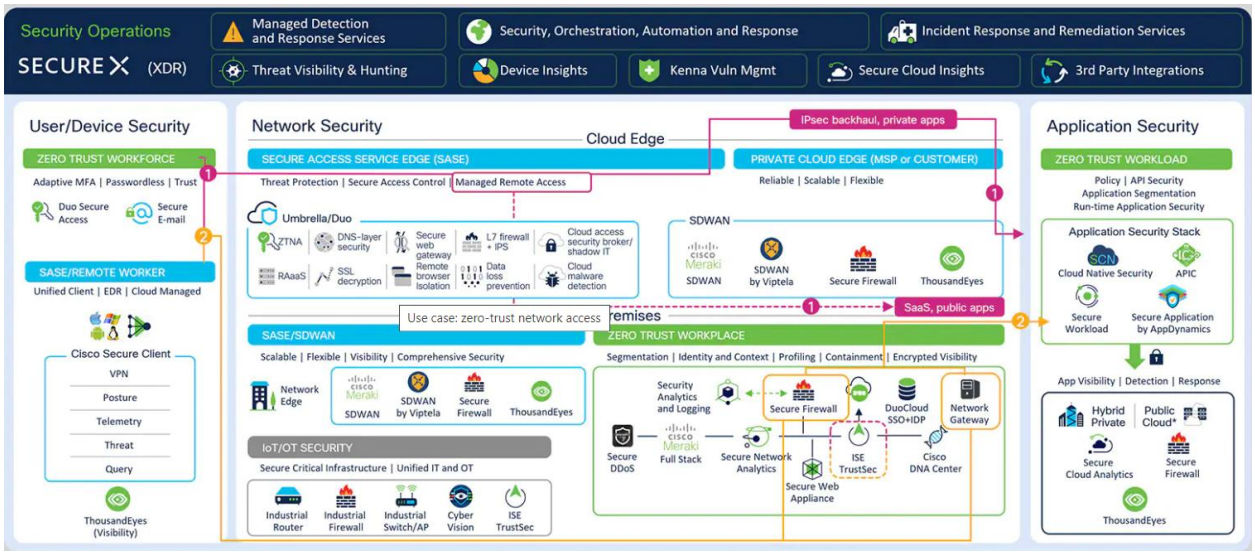

Рисунок 2.5 – Доступ до мережі з нульовою довірою

Рішення Cisco Zero Trust забезпечує безпеку користувачів і програм у всій архітектурі. І персональні пристрої BYOD, і корпоративні пристрої

проходять адаптивну багатофакторну аутентифікацію та призначають найменш привілейований доступ із безперервним моніторингом довіри. Доступ до програми динамічно скасовується або авторизується, якщо статус положення користувача/пристрою змінюється. За допомогою керованого ZTNA від Umbrella клієнти можуть розвантажити адміністрування віддаленого доступу до керованих служб Cisco і швидко розгорнути служби з нульовою довірою для захисту публічних і приватних програм. Клієнти ZTNA, які самостійно керують, можуть продовжувати розгортати послуги AnyConnect VPN або використовувати хмарний єдиний вхід (single sign-on (SSO)) Duo і мережевий шлюз Duo для доступу до додатків, не заснованих на VPN. Система єдиного входу Duo без пароля покращує та спрощує вхід користувачів.

На рисунку 2.6 наведено приклад SecureX оркестрування та телеметрію.

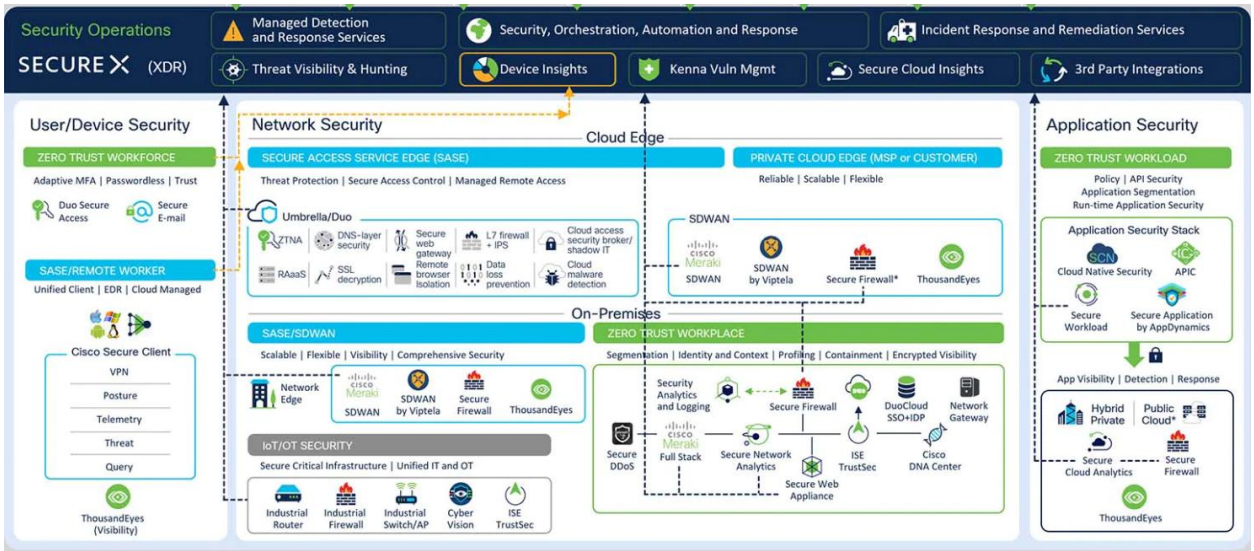

Рисунок 2.6 – Приклад SecureX телеметрії та оркестрування

Платформа Cisco SecureX забезпечує видимість, розслідування/реагування та організацію з обміном інформацією про контекст і загрози, щоб допомогти особам, які реагують на інциденти. Інформацію про кінцевий пристрій (починаючи від керування мобільними

пристроями, програмного забезпечення для захисту кінцевих точок, наприклад Duo Device Health, клієнтів Cisco Secure і керування антивірусними програмами сторонніх виробників) можна надсилати до Device Insights для повної інвентаризації активів та перевірки відповідності. Відкриті та гнучкі можливості API SecureX ще більше підвищують ефективність загроз через інтеграцію сторонніх розробників. Оркестровка SecureX дозволяє адміністраторам звертатися з хмари до корпоративних мереж, щоб застосувати правило блокування або політику всередині корпоративних брандмауерів або інших пристроїв, що примушують до виконання.

2.4 Захист мереж за допомогою брандмауерів

Брандмауери існували з кінця 1980-х років і починалися як фільтри пакетів, які являли собою мережі, створені для перевірки пакетів або байтів, переданих між комп'ютерами. Хоча брандмауери фільтрації пакетів використовуються і сьогодні, брандмауери пройшли довгий шлях, оскільки технології розвивалися протягом десятиліть [46-50].

Покоління 1, кінець 1980-х років, вірусні атаки на автономні комп'ютери вплинули на всі підприємства та викликали антивірусні продукти.

Покоління 2, середина 1990-х років, атаки з Інтернету вплинули на весь бізнес і спричинили створення брандмауера.

Покоління 3, початок 2000-х, використовувало вразливості в програмах, які вплинули на більшість компаній і привели до створення продуктів систем запобігання вторгненням (IPS).

Покоління 4, прибл. 2010 р., зростання цілеспрямованих, невідомих, унікальних, поліморфних атак, які вплинули на більшість компаній і викликали продукти для боротьби з роботами та пісочницями.

Покоління 5, приблизно з 2017 року, широкомасштабні багатовекторні, мегаатаки з використанням інструментів передових атак стимулюють рішення для запобігання загрозам.

Типи брандмауерів можна визначити як наступні:

– пакетна фільтрація. Невелика кількість даних аналізується і розподіляється відповідно до стандартів фільтра;

– проксі-сервіс. Система безпеки мережі, яка захищає під час фільтрації повідомлень на прикладному рівні;

– державна перевірка. Динамічна фільтрація пакетів, яка відстежує активні з'єднання, щоб визначити, які мережеві пакети дозволити через брандмауер.

– брандмауер наступного покоління (Next Generation Firewall NGFW). Глибока перевірка пакетів брандмауер з перевіркою на рівні програми.

Брандмауер є необхідною частиною будь-якої архітектури безпеки і переносить функції засобів захисту на рівні хоста до пристроїв безпеки мережі. Брандмауери, і особливо брандмауери наступного покоління, зосереджені на блокуванні зловмисного програмного забезпечення та атак на рівні програм, разом з інтегрованою системою запобігання вторгненням (IPS), можуть швидко та плавно реагувати, виявляючи зовнішні атаки по всій мережі та реагуючи на них. Вони можуть встановлювати політику для кращого захисту вашої мережі та виконувати швидкі оцінки, щоб виявити інвазивну або підозрілу активність, як-от зловмисне програмне забезпечення, та закрити її.

Мережевий рівень або фільтри пакетів перевіряють пакети на відносно низькому рівні стеку протоколів TCP/IP, не дозволяючи пакетам проходити через брандмауер, якщо вони не відповідають встановленому набору правил, де джерело та призначення набору правил засновані на IP-адресі та номеру порта. Брандмауери, які здійснюють перевірку мережевого

рівня, працюють краще, ніж аналогічні пристрої, які здійснюють перевірку рівня програм. Недоліком є те, що небажані програми або шкідливі програми можуть проходити через дозволені порти, напр. вихідний інтернет-трафік по веб-протоколах HTTP і HTTPS, порт 80 і 443 відповідно.

Брандмауери також виконують основні функції мережевого рівня, такі як трансляція мережевих адрес (NAT) і віртуальна приватна мережа (VPN). Трансляція мережевих адрес приховує або перекладає внутрішні IP-адреси клієнта або сервера, які можуть бути в “приватному діапазоні адрес”, як визначено в RFC 1918, на загальнодоступну IP-адресу. Приховування адрес захищених пристроїв зберігає обмежену кількість адрес IPv4 і є захистом від розвідки мережі, оскільки IP-адреса прихована від Інтернету.

Аналогічно, віртуальна приватна мережа (VPN) розширює приватну мережу через загальнодоступну мережу в тунелі, який часто шифрується, де вміст пакетів захищений під час проходження Інтернету. Це дозволяє користувачам безпечно надсилати та отримувати дані через спільні чи загальнодоступні мережі.

Більшість операційних систем рішення брандмауера все-в-одному забезпечені постачальником. Якщо ви розгортаєте програмне рішення брандмауера, переконайтеся, що ОС спочатку виправлена та посилена останніми оновленнями.

Окрім того, що починати з посиленої оновленнями ОС, адміністратори безпеки захочуть переконатися, що брандмауер безпечно налаштований. Рекомендації доступні від постачальників і третіх сторін, наприклад, Центр безпеки в Інтернеті (CIS), який публікує контрольні показники мережевих пристроїв CIS. Також доцільно переглянути контрольний список брандмауера SANS.

Брандмауери є важливим інструментом для застосування принципів безпеки без довіри. Вони відстежують і контролюють вхідний і вихідний доступ через межі мережі в макросегментованій мережі. Це стосується як

розгортань брандмауера з маршрутизацією рівня 3 (де брандмауер діє як шлюз, що з'єднує кілька мереж), так і розгортань брандмауера моста рівня 2 (де брандмауер з'єднує та ізолює пристрої в одній мережі).

Під час розгортання брандмауера мережеві інтерфейси брандмауера підключаються до цих мереж або зон. Ці зони потім можна використовувати для спрощення політики брандмауера. Наприклад, брандмауер периметра матиме зовнішню зону, підключену до Інтернету, один або кілька внутрішніх інтерфейсів, підключених до внутрішніх мереж, і, можливо, мережеве з'єднання DMZ. Потім політику брандмауера можна налаштувати за потреби, щоб додати більш детальний контроль.

Нарешті, один брандмауер є єдиною точкою відмови. Розгортання двох або більше в кластері високої доступності гарантує безпеку продовження в разі збою одного. Кращим варіантом, який постійно використовує ресурси кожного члена кластера, є гіпермасштабне рішення безпеки мережі. Це також слід враховувати для мереж, де навантаження на трафік має сезонні піки.

Брандмауер є важливим компонентом інфраструктури безпеки організації, і його потрібно захищати від використання. Щоб захистити свій брандмауер, виконайте такі дії:

– вимкніть незахищені протоколи, такі як telnet і SNMP, або використовуйте безпечну конфігурацію SNMP;

– плануйте періодичне резервне копіювання конфігурації та бази даних;

– увімкніть аудит системних змін і надсилайте журнали через захищений системний журнал або іншим способом на зовнішній захищений центральний сервер SIEM або рішення для керування брандмауером для криміналістики та звітності;

– додайте правило прихованості в політику брандмауера, щоб приховати брандмауер від сканування мережі;

– обмежте доступ керування для певних хостів;

– брандмауери не застраховані від вразливостей. Зверніться до постачальника, щоб дізнатися, чи є якісь відомі вразливості та виправлення безпеки, які усувають уразливість.

Захоплення облікового запису є поширеною технікою, яку використовують суб'єкти кіберзагроз. Щоб захистити облікові записи користувачів у вашому брандмауері, виконайте такі дії:

– перейменуйте або змініть облікові записи та паролі за замовчуванням;

– вимагати MFA та/або встановлювати надійну політику паролів (складні паролі з великими та малими літерами, спеціальними символами та цифрами, 12 символів або більше, запобігають повторне використання паролів);

– використовуйте контроль доступу на основі ролей (role-based access control RBAC) для адміністраторів брандмауера. Делегувати та обмежувати доступ відповідно до потреб користувача в доступі (тобто дозволяти аудиторам доступ лише для читання та створювати спеціальні ролі та облікові записи для команд DevSecOps)

Основною функцією брандмауера є забезпечення та моніторинг доступу для сегментації мережі.

Брандмауери можуть перевіряти та контролювати трафік північ/південь через кордон мережі. У цьому випадку використання макросегментації зонами створює широкі групи, такі як зовнішні, внутрішні, DMZ та гостьовий Wi-Fi. Вони також можуть бути бізнес-групами в окремих внутрішніх мережах, таких як центр обробки даних, відділ кадрів та фінансів, або виробничий цех на виробничому підприємстві, який використовує системи промислового контролю (ICS).

Брандмауери, розгорнуті у віртуалізованих приватних або загальнодоступних хмарах, можуть перевіряти трафік між окремими

серверами або програмами, які динамічно змінюються в міру створення екземплярів. У цьому випадку відбувається затсосування мікросегментації і зони можуть бути визначені такими програмами, як веб-програми або бази даних. Функція віртуального сервера може встановлюватися тегом і використовуватися в політиці брандмауера динамічно без втручання людини, зменшуючи ймовірність помилок конфігурації вручну.

В обох розгортаннях, макро та мікро, брандмауери контролюють доступ, встановлюючи правило політики брандмауера, яке широко визначає доступ на основі джерела та призначення трафіку. Також можна визначити службу або порт, який використовує програма. Наприклад, порти 80 і 443 є портами за замовчуванням для веб-трафіку. На веб-сервері має бути дозволений доступ лише до цих портів, а всі інші порти заблоковані. Це той випадок, коли можливий білий список дозволеного трафіку.

Вихідний трафік від організації до Інтернету є більш проблематичним для політики безпеки до білого списку, оскільки майже неможливо сказати, які порти потрібні для доступу до Інтернету. Більш поширеним підходом до політики безпеки виходу є чорний список, де відомий поганий трафік блокується, а все інше дозволяється за допомогою правила політики брандмауера “прийняти всі”.

Щоб виявити відомі погані сайти, додаткові функції безпеки можна ввімкнути на брандмауері нового покоління (NGFW) на додаток до засобів керування IP-адресами та портами. До них відноситься фільтрація URL-адрес і контроль програм. Наприклад, це можна використовувати, щоб дозволити доступ до Facebook, але блокувати ігри Facebook.

Правила мають особливі вимоги до брандмауерів. Будь-яка найкраща практика безпеки повинна відповідати цим вимогам і може вимагати додавання додаткових засобів контролю безпеки до будь-якого розгорнутого брандмауера. Приклади вимог включають використання віртуальних приватних мереж (VPN) для шифрування даних під час передачі,

антивірусної програми для запобігання відомим шкідливим програмним забезпеченням та систем виявлення та запобігання вторгненням (IDS/IPS) для виявлення будь-яких спроб вторгнення в мережу.

Наприклад, PCI DSS вимагає керування зонами між довіреними та ненадійними зонами на основі брандмауера. Це включає використання DMZ та брандмауерів периметра між усіма бездротовими мережами та середовищами даних власників карток. Деякі додаткові вимоги PCI DSS включають:

– використовуйте засоби захисту від спуфінгу для виявлення та блокування доступу до мережі фальсифікованих вихідних IP-адрес. Наприклад, блокувати вхідний трафік на зовнішньому інтерфейсі з адресою джерела однієї з внутрішніх мереж;

– не розголошувати приватні IP-адреси та інформацію про маршрутизацію неавторизованим особам за допомогою трансляції мережевих адрес (NAT) та видалення реклами маршрутів для приватних мереж;

– кожні півроку очищайте всі непотрібні, застарілі чи помилкові правила та переконайтеся, що всі набори правил дозволяють виключно авторизовані служби та порти;

– шифруйте передачу даних власників карток через відкриті загальнодоступні мережі;

– встановіть відповідні виправлення безпеки, надані постачальником. Установіть важливі виправлення безпеки протягом одного місяця після випуску. (З огляду на те, як швидко суб’єкти загроз використовують відомі вразливості, компанії можуть захотіти змінити це, щоб оновити, коли буде доступний патч. NGFW, який автоматично оновлює підписи IPS, може захистити цілі мережі від нещодавно оголошених уразливостей.);

– повинні бути встановлені процеси для обмеження доступу на основі вимог знань та відповідно до посадових обов’язків;

– відстежуйте та контролюйте весь доступ до мережевих ресурсів і даних власників карток;

– використовуючи технологію синхронізації часу, синхронізуйте всі важливі системні годинники та час.

– регулярно тестуйте системи та процеси безпеки.

З більшою політикою безпеки може бути важко уявити, як вона оброблятиме нове з'єднання. Існують інструменти для аналізу шляхів, що можуть існувати в системі управління безпекою для пошуку правил.

Крім того, деякі системи керування безпекою попереджають, коли створюється повторюваний об'єкт або не встановлюють політику, яка має правило, яке приховує інше. Регулярно перевіряйте свою політику, щоб переконатися, що вона працює належним чином, щоб знайти невикористані та повторювані об'єкти.

Політики брандмауера зазвичай застосовуються в порядку зверху вниз, і їх можна оптимізувати, переміщаючи правила звернення догори вгору в порядку перевірки. Регулярно перевіряйте політику, щоб оптимізувати роботу брандмауера.

Нарешті, виконуйте регулярне тестування на проникнення, щоб виявити ризики, додаткові заходи безпеки, які можуть знадобитися на додаток до брандмауера для захисту організації.

Регулярні перевірки необхідні, щоб переконатися, що програмне та мікропрограмне забезпечення є правильними та оновленими, а журнали правильно налаштовані та працюють. Нижче наведено кілька найкращих методів проведення таких аудитів:

– створіть офіційний план контролю змін для зміни політики безпеки, щоб гарантувати, що безпека не буде порушена;

– правила з будь-яким набором у джерелі, призначенні або порті можуть бути дірками в політиці безпеки. Якщо можливо, змініть їх, щоб додати конкретне джерело, призначення або службу, що є метою правила;

– створіть розділи або шари, щоб додати ієрархію до політики безпеки, що полегшить перегляд;

– додайте правила очищення в кінець розділу або шару, які відповідають намірам шару (тобто дозволити все чи заборонити все);

– додайте коментарі та назви до правил, щоб допомогти визначити початкову мету кожного правила;

– увімкніть ведення журналів, щоб краще відстежувати мережеві потоки та додати видимість для судово-медичних розслідувань і звітів;

– регулярно переглядайте журнали аудиту та звіти, щоб дізнатися, хто змінив політику брандмауера.

Використання загальних підходів та рекомендацій щодо роботи брандмауре на основі зон суттєво захищає мережеві ресурси та покращує роботу мережі.

2.5 Методи та засоби підвищення захисту мережі

Завдяки революції віддаленої роботи майбутнє безпеки стане ефективнішим, надійнішим і зручнішим для користувачів та можливо, навіть без пароля [51-54].

Вигляд аутентифікації явно змінюється. Всього кілька років тому експерти з безпеки почали проповідувати модель доступу, що ґрунтується на ризиках – оцінюючи користувачів, їхні пристрої та програми, до яких вони мають доступ, щоб визначити легітимність входу. Корпоративна мережа більше не була основним джерелом безпеки. Натомість ризиком можна керувати за допомогою посилених засобів контролю безпеки, таких як багатофакторна аутентифікація (multi-factor authentication (MFA)).

Тепер, коли концепція деперіметризації міцно закріпилася, безпека доступу будується на основі MFA. IT-фахівці розуміють, що впровадження безпеки настільки ж важливе, як і сама технологія, і що відмова від паролів є

значним покращенням зручності використання. Зрозуміло також, що віддалена робота залишиться популярною, а безпека доступу повинна реагувати на нові та розвинуті варіанти застосування. З огляду на такі великі зміни, як ніколи важливо, щоб організації мали впорядкований, ефективний стек безпеки, що працює як годинник.

Більш ніж будь-коли організації усвідомлюють, що зручність використання – це безпека. Робочі процеси безпеки, якими легко орієнтуватися, з більшою ймовірністю будуть прийняті і рідше будуть зламані, тому цінність добре розробленого інтерфейсу не можна недооцінювати.

Акцент на досвіді очевидний у даних аутентифікації Duo – помічено, що використання зручних для користувача методів аутентифікації, таких як біометричні дані, WebAuthn і Duo Push, значно зросло з 2019 року.

На рисунку 2.7 показно зміни методів автентифікації в період з 2019 до 2021 року.

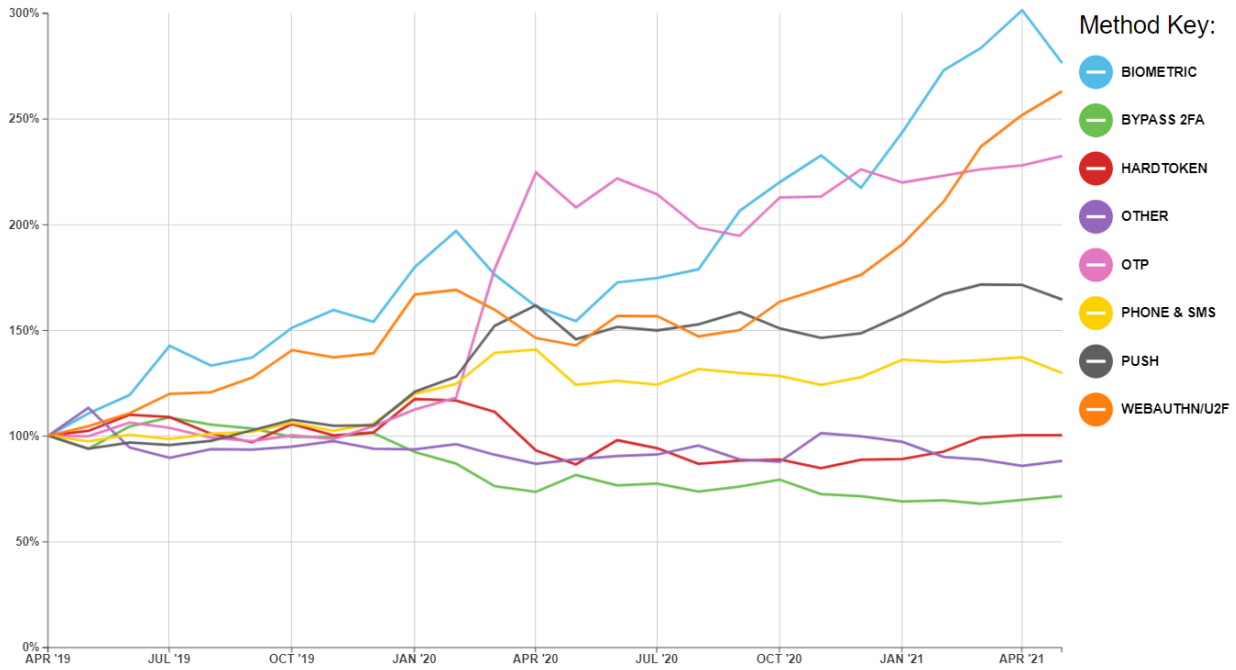

Рисунок 2.7 – Зміна методів автентифікації 2019-2021 роки

Організації демонструють відхід від паролів, що значно покращить досвід входу для багатьох користувачів. Нещодавно Cisco провела опитування тих, хто приймає технічні рішення з усього світу, і виявила, що понад 50% розглядають рішення без пароля. Коли їх попросили вибрати головні критерії, особи, які приймають рішення, постійно визначали підвищення загальної безпеки своєї компанії та покращення досвіду кінцевих користувачів як найважливіше.

За результатами опитування проведеного компанією Duo складено відношення реалізації безпарольної автентифікації у різних країнах.

На рисунку 2.8 показно як останні технології автентифікації вплинули на досвід користувачів у різних країнах.

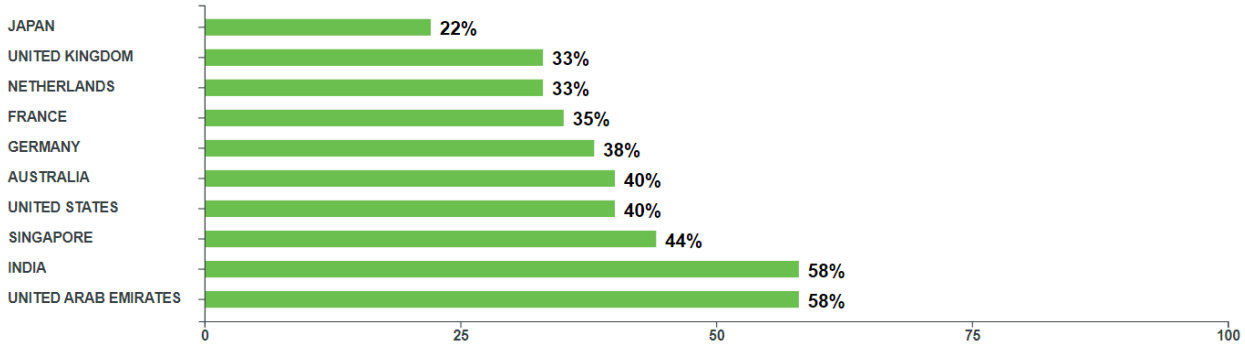

Рисунок 2.8 – Порівняльний аналіз впливу технології автентифікації

Як видно з поданого матеріалу, у розвинених країнах відсоток впливу меньший за рахунок попередньо впроваджених високих технологій, а у країнах з меньшим розвитком він суттєвіший.

На рисунку 2.9 подано темпи нарощування впроваджування безпарольної автентифікації. Аналіз поданого матеріалу показує, що країни які почали впроваджувати сучасні технології раніше сповільнюють темп за рахунок глибокого проникнення даних послуг. В свою чергу інші країни планомірно продовжують роботу щодо забезпечення використання безпарольного доступу до ресурсів мережі.

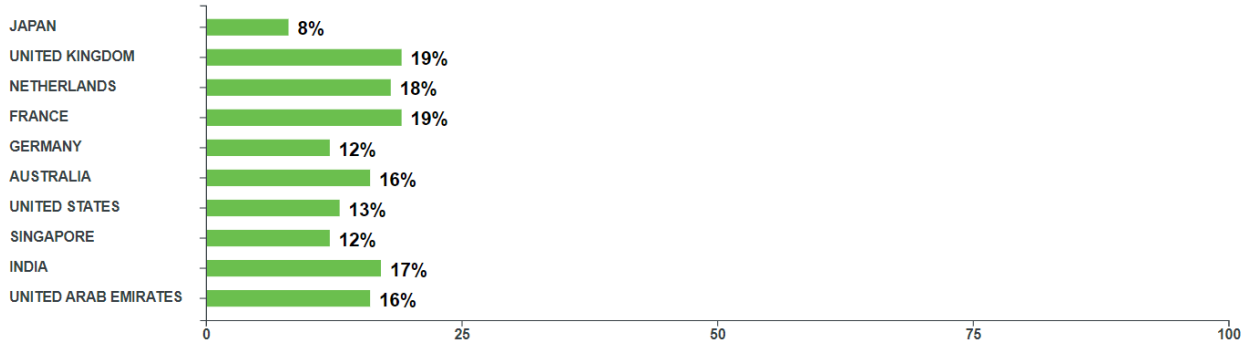

Рисунок 2.9 – Темпи нарощування впровадження безпарольної автентифікації

На рисунку 2.10 показано позитивну динаміку покращення автентифікації при використанні безпарольного входу.

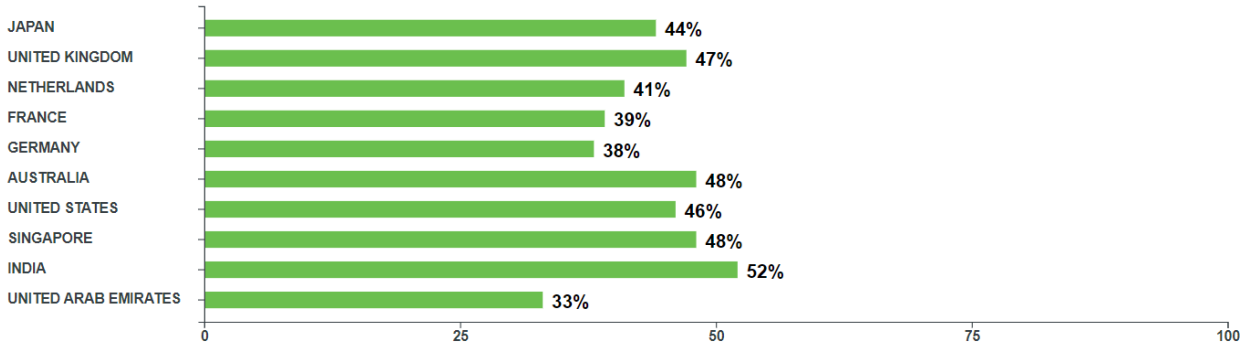

Рисунок 2.10 – Покращення автентифікації через використання безпарольного входу

Як видно з поданого матеріалу, більшість країн показують позитивну динаміку покращення захисту ресурсів мережі через використання безпарольної автентифікації.

Безпарольну автентифікацію можна досягти багатьма способами. Наведемо кілька прикладів:

– біометрія: фізичні ознаки, такі як сканування відбитків пальців або сітківки ока, а також поведінкові риси, як-от введення тексту та динаміка сенсорного екрана, використовуються для однозначної ідентифікації людини. Незважаючи на те, що сучасний штучний інтелект дозволив хакерам

підробити певні фізичні риси, поведінкові характеристики все ще дуже важко підробити;

– фактори володіння: автентифікація за допомогою чогось, що є у користувача або того, що він носить з собою. Наприклад, код, згенерований програмою для аутентифікації смартфона, одноразові паролі, отримані через SMS, або апаратний маркер.

– чарівні посилання: користувач вводить свою електронну адресу і система надсилає йому електронний лист. Електронний лист містить посилання, натискання на яке надає користувачеві доступ.

На рисунку 2.11 показано динаміку зміни користувацького досвіду від впровадження безпарольної автентифікації.

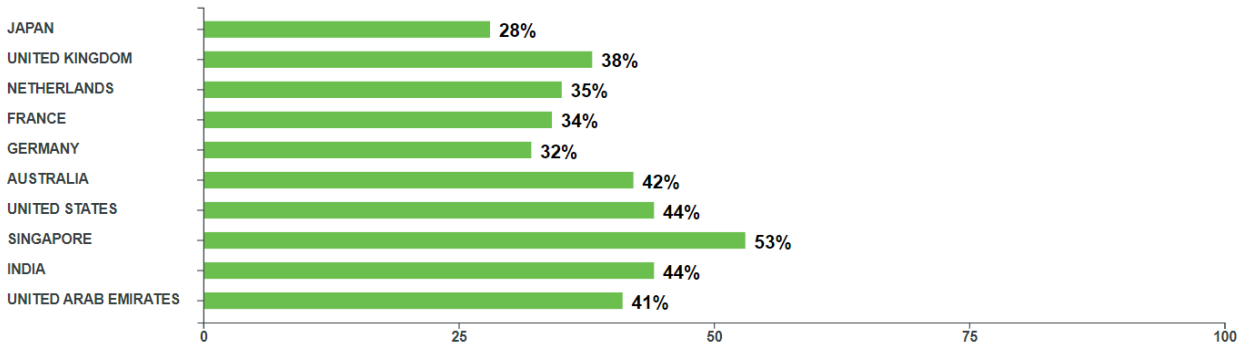

Рисунок 2.11 – Динаміка зміни користувацького досвіду від впровадження безпарольної автентифікації

Незважаючи на те, що паролі є набагато менш поширеними, ніж будь-коли раніше, вони все ще використовуються у всьому світі. Основна причина полягає в тому, що система входу на основі пароля є найпростішою та найдешевшою у реалізації. Однак очікується, що безпарольний етап незабаром почнеться.

За останні два роки було більше кібератак, ніж будь-коли раніше. Це викликає тривогу у багатьох компаніях, де все більше вкладається в біометричні дані та адаптивну аутентифікацію.

Більше того, зараз багато компаній зрозуміли, що паролі є основною причиною злому даних. Вартість впровадження безпарольної системи ніщо в порівнянні зі штрафами та втратами, понесеними через порушення даних.

І останнє, але не менш важливе, паролі заважають користувачам. Важко запам’ятати складні паролі і постійно їх міняти. З іншого боку, безпарольні методи, такі як біометричні, зручні та набагато інтуїтивно зрозуміліші для користувачів.

Незважаючи на те, що аутентифікація без пароля є значною перевагою в порівнянні з використанням паролів, вона все ще не безпомилкова. Біометричні дані можуть бути підроблені, одноразові паролі можуть бути перехоплені, а апаратні токени можуть бути вкрадені. Ось чому потрібна система, яка виходить за рамки просто факторів аутентифікації для перевірки ідентичності і проводить адаптивну автентифікацію.

Адаптивна автентифікація використовує машинне навчання для розробки моделей типової поведінки користувача. Кожного разу, коли система помічає відхилення від шаблону, вона розглядає спробу входу як ризиковану та вживає відповідних дій.

Наприклад, припустимо, що користувач входить в систему через свій ноутбук рано вранці, кожного буднього дня. З часом система визначає, що це типова поведінка входу. Потім одного дня користувач входить в систему в суботу. Користувач використовує той самий ноутбук, який був ще вранці і географічне розташування також було таким же. Система обчислює відносно вищий показник ризику для такої поведінки, що виправдовує використання вторинного фактора аутентифікації такого як SMS OTP.

Через кілька днів система помічає спробу входу від того самого користувача з іншої країни та іншого пристрою. Вона обчислює експоненціально вищий показник ризику та блокує користувача. Пізніше з’ясувалося, що це була спроба входу в систему від кіберзлочинця, який підробив особистість користувача.

Поєднання безпарольної автентифікації з адаптивною автентифікацією може зробити систему набагато більш стійкою. Зламати фактори без пароля важче, але не неможливо. В той же час адаптивна автентифікація допомагає додати ще один рівень захисту на основі штучного інтелекту.

2.6 Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений організації зонової безпеки комп’ютерної мережі. Для цього в даному розділі подано індикатори вторгнення, що дають змогу на основі типових характеристик втручання розробляти відповідні методи та засоби захисту. Запропоновано використання глибокого тестування мережі для виявлення слабкостей та їх усунення. Подано основні архітектурні рішення забезпечення захисту мережі на основі зон. У логічній архітектурі узагальнено використання типових підходів організації безпечної роботи мережі. На основі досвіду провідних компаній показано комплексні міри та рішення організації зонової безпеки комп’ютерної мережі. Визначено роль хмарних сервісів в організації безпеки зон для різних сценаріїв. Запропоновано використання брандмауерів та надано рекомендації щодо впровадження даних засобів для їх ефективної роботи. Проведено аналіз можливості застосування методів підвищення захисту мереж на основі безпарольної автентифікації, що показує майбутні напрямки розвитку технології для забезпечення зонової безпеки критичних інфраструктур.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Безпечні умови праці при монтажі комп'ютерної мережі

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: "Про охорону праці", "Про охорону здоров'я", "Про пожежну безпеку".

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2006 [55].

Згідно з ДСанПіН 3.3.2-007-98 [56] та з Правилами охорони праці під час експлуатації ЕОМ НПАОП 0.00-1.28-10 [57] площа на одне робоче місце має становити не менше ніж 6,0 кв. м, а об'єм – не менше ніж 20,0 куб. м

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Особи з простудними і хронічними захворюваннями верхніх дихальних шляхів до роботи з монтажу комп'ютерних мережі та заготовки і монтажу пластмасових труб не допускаються.

Згідно ДНАОП 0.00-1.15-07 [58]. Правила охорони праці під час виконання робіт на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів. До виконання робіт на висоті допускаються особи, не молодше 18 років, та які пройшли:

– професійний добір відповідно до Переліку робіт, де є потреба у професійному доборі, затвердженого спільним наказом Міністерства охорони здоров'я України та Державного комітету України з нагляду за охороною праці від 23.09.94 N 263/121, зареєстрованого в Міністерстві юстиції України 25.01.95 за N 18/554;

– медичний огляд відповідно до вимог Положення про медичний огляд працівників певних категорій, затвердженого наказом Міністерства охорони здоров'я України від 31.03.94 N 45, зареєстрованого в Міністерстві юстиції України 21.06.94 за N 136/345;

– спеціальне навчання та перевірку знань з охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Державного комітету України з нагляду за охороною праці від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 (далі - НПАОП 0.00-4.36-05 [59]).

Вимоги безпеки перед початком роботи передбачають, що до початку робіт з монтажу комп’ютерної мережі керівник зобов’язаний:

– перевірити ступінь готовності будівельних робіт;

– оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду; можливість безпечного застосування піротехнічного інструменту, безпечної подачі електричних конструкцій, електротехнічних апаратів та інших блоків;

– узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

– ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Керівник робіт повинен здійснити первинний інструктаж, який стосується:

– характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

– наявності небезпечних зон та відкритих каналів і траншей, відкритих прорізів, отворів у перекриттях та стінах;

– порядку розвантаження та складування матеріалів, устаткування та конструкцій;

– місць та порядку трансформаторів безпеки, електрифікованого інструменту, засобів електроосвітлення, випробувальних апаратів;

– порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

– надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежобезпеки, посвідчень на право виконання спеціальних видів робіт (зварювання, монтаж кабельної арматури).

Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов’язкові.

Попередити працюючих, що з’єднання та від’єднання від мережі обладнання, механізмів, інструменту, інвентарних шаф тощо (крім оперативного вмикання і вимикання) в умовах будівельного майданчика виконуються тільки службою експлуатації власника мережі, якщо не існує іншої письмової домовленості з власником.

Вимоги безпеки під час виконання роботи:

– прокладання кабелів слід виконувати тільки в рукавицях.

– працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

– переносити чи перевозити інструмент з гострими кутами треба лише в чохлах.

– не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї.

– перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана.

– переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше .

Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку. Перед розмотуванням барабан встановити на домкрати (чи інший підіймальний пристрій). Барабан встановити так, щоб кабель розмотувався з його верхньої частини. Розмотувати кабель з барабана слід тільки за наявності гальмівного пристрою.

Прокладання кабелів і монтаж мережевого обладнання слід виконувати у захисному одязі з можливістю використання електростатичних браслетів.

Згідно ДБН В.2.5-23:2010 [60]. Проектування електрообладнання об'єктів цивільного призначення установлена потужність робочого місця локальної обчислювальної мережі (ЛОМ) (без врахування периферійних пристроїв) приймається 250...300 Вт, сервера – 750... 1000 Вт або згідно з технічною документацією на ці електронні пристрої ЛОМ.

Граничні значення Х електронних пристроїв різної потужності для закордонних виробників обмежується стандартом EN 61000-3-2, для більшості випадків значення можливо приймати 0,72.

Усі об’єкти ЛОМ мають як активну, так і реактивну складові навантаження, тобто повна потужність у вольт-амперах (ВА, англ. «VA») і активна потужність у ватах (Вт, англ. «W») зв’язані між собою коефіцієнтом cos φ. На приладах (блоці живлення комп’ютера) вказують їхню активну

споживану потужність у ватах. Щоб підрахувати повну потужність у ВА, потрібно активну потужність у Вт розділити на cos φ. Наприклад, якщо на блоці живлення комп'ютера написано «850 Вт» (cos φ зазвичай не вказаний), це означає, що для грубого розрахунку повної потужності, яка споживається насправді, можна активну потужність розділити на 0,7. Споживана повна потужність дорівнюватиме 850 Вт/0,7 ≈ 1200 ВА = 1,2 кВА. Необхідно визначити суму потужностей усіх споживачів, що мають потребу в одночасному постачанні електроенергії.

При проектуванні електрообладнання будинків та споруд слід також керуватись вимогами відповідних розділів правила улаштування електроустановок (ПУЕ), розділів 2, 3, 4.1, 4.2, 9 [61], та нормативно-правових актів охорони праці (НПАОП) 40.1-1.32 [62] та вимогами інших чинних нормативних документів.

Не можна застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, які містять сірку. У всіх приміщеннях із серверами та робочими місцями, обладнаними ЕОМ, повинні бути встановлені переносні вуглекислотні вогнегасники. Використання води для гасіння пожежі в приміщеннях, де встановлено електро- і радіоелектронне обладнання, недопустиме, не можна також користуватись і кислотно-лужними вогнегасниками. У громадських будинках та приміщеннях з наявністю ПЕОМ, приміщеннях обчислювальних центрів рекомендується використовувати вуглекислотні вогнегасники типу ОУ-5, ОУ-8, ОУ-25, ОУ-80, вуглекислотні бром-етилові вогнегасники типу ОУБ-3 і ОУБ-7, вуглекислотні вогнегасники від ВВК-1 до ВВК-5, які придатні до експлуатації при температурі повітря від мінус 20 до плюс 50°С.

Кількість вогнегасників для захисту приміщень визначають згідно з п. 3.8 норм належності, затверджених МНС України, та з урахуванням сумарної площі цих приміщень. Тобто слід передбачати по одному вуглекислотному вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше на

кожні 20 кв. м площі підлоги в офісних приміщеннях із ПЕОМ та електрощитових і на 50 кв. м площі підлоги приміщень машзалів.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-56:2010 [63]. Установки порошкового пожежогасіння не застосовують для захисту приміщень із ЕОМ, апаратних залів АТС та інших приміщень із великою кількістю відкритих контактних пристроїв.

У приміщенні, де одночасно експлуатуються понад п’ять ЕОМ з ВДТ і ПП, на доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Електромережі штепсельних з’єднань та електророзеток для живлення ЕОМ з ВДТ і ПП потрібно будувати за магістральною схемою, по 3 – 6 з’єднань або електророзеток в одному колі.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Ультразвук та інфразвук, його вплив на організм людини

Ультразвук являє собою механічні коливання пружного середовища, що мають однакову зі звуком фізичну природу, але відрізняються більш високою частотою, що перевищує прийняту верхню межу чутності - понад 20 кГц, хоча при великих інтенсивностях (120 ... 145 дБ) чутними можуть бути і звуки більш високої частоти.

Ультразвук, як і звук, характеризується ультразвуковим тиском (Па), інтенсивністю (Вт/м2) і частотою коливань (Гц).

При поширенні в різних середовищах ультразвукові хвилі поглинаються, причому тим більше, чим вище їх частота. Низькочастотний ультразвук досить добре розповсюджується в повітрі, а високочастотний - практично не поширюється. У пружних середовищах (воді, металі та ін)

ультразвук мало поглинається і здатний поширюватися на великі відстані, практично не втрачаючи енергії. Поглинання ультразвуку супроводжується нагріванням середовища.

Специфічною особливістю ультразвуку, обумовлене великою частотою і малою довжиною хвилі, є можливість поширення ультразвукових коливань спрямованими пучками, які отримали назву ультразвукових променів. Вони створюють на відносно невеликій площі дуже велике ультразвукове тиск. Це властивість ультразвуку зумовило широке його застосування: для очищення деталей, механічної обробки твердих матеріалів, зварювання, пайки, прискорення хімічних реакцій, дефектоскопії, перевірки розмірів виробів, що випускаються, структурного аналізу речовин, гідролокації та ін Знайшов застосування ультразвук і в медицині для лікування захворювань хребта, суглобів, периферичної нервової системи.

При тривалій роботі з низькочастотними ультразвуковими установками, що генерують шум і ультразвук, що перевищують встановлені, можуть відбутися функціональні зміни центральної і периферичної нервової системи, серцево-судинної системи, слухового і вестибулярного апарату і т. п. У порівнянні з високочастотним шумом ультразвук значно слабше впливає на слухову функцію, але викликає більш виражені відхилення від норми вестибулярної функції, больової чутливості і терморегуляції. Те, що ультразвук впливає на різні органи і системи людини не тільки через слуховий апарат, підтверджується несприятливим його дією на глухонімих.

Для колективного захисту від дії підвищених рівнів ультразвуку можна використовувати такі напрями: зменшення шкідливого випромінювання ультразвукової енергії в джерелі її виникнення; локалізацію дії ультразвуку конструктивними і планувальними рішеннями, проведення організаційно-профілактичних заходів.

Для зменшення шкідливого випромінювання звукової енергії в джерелі рекомендується підвищувати робочі частоти джерел ультразвуку, що

забезпечує зменшення інтенсивності ультразвуку, а також виключати паразитні випромінювання звукової енергії.

Для локалізації ультразвуку обов'язковим є застосування звукоізолюючих кожухів, екранів. Якщо ці заходи не дають позитивного ефекту, то ультразвукові установки потрібно розміщувати в окремих приміщеннях і кабінах, облицьованих звукопоглинальними матеріалами.

Контактний вплив ультразвуку виключається автоматизацією виробничих процесів і застосуванням дистанційного управління. При особливої необхідності використовують спеціальний інструмент з віброізолюючий рукояткою і захисні рукавички.

Організаційно-профілактичні заходи полягають у проведенні інструктажу працюючих та встановлення раціональних режимів праці та відпочинку.

Інфразвук являє собою механічні коливання пружного середовища, що мають однакову з шумом фізичну природу, але поширюються з частотами менше 20 Гц. У повітрі інфразвук мало поглинається і тому здатний поширюватися на великі відстані. Інфразвук характеризується інфразвукових тиском (Па), інтенсивністю (Вт/м2), частотою коливань (Гц). Рівні інтенсивності інфразвуку і інфразвукового тиску виражаються в децибелах (дБ). Багато явищ природи (землетруси, виверження вулканів, морські бурі) супроводжуються випромінюванням інфразвукових коливань. У виробничих умовах інфразвук утворюється, головним чином, при роботі тихохідних великогабаритних машин і механізмів (компресорів, дизельних двигунів, електровозів, вентиляторів, турбін, реактивних двигунів і ін), які роблять обертальний або зворотно-поступальний рух з повторенням циклу менше ніж 20 разів на секунду (інфразвук механічного походження). Інфразвук аеродинамічного походження виникає при турбулентних процесах у потоках газів чи рідин.

Інфразвук справляє негативний вплив на весь організм людини, в тому числі і на орган слуху, знижуючи слухову чутливість на всіх частотах. Інфразвукові коливання сприймаються як фізичне навантаження: виникають стомлення, головний біль, запаморочення, вестибулярні порушення, знижується гострота зору і слуху, порушується периферичний кровообіг, з'являється відчуття страху і т. п. Тяжкість впливу залежить від діапазону частот, рівня звукового тиску і тривалості.

Низькочастотні коливання з рівнем інфразвукового тиску понад 150 дБ зовсім не переносяться людиною. Особливо несприятливі наслідки викликають інфразвукові коливання з частотою 2 ... 15 Гц у зв'язку з виникненням резонансних явищ в організмі людини, причому найбільш небезпечна частота 7 Гц, так як можливо його збіг з альфа-ритмом біострумів мозку.

Згідно з СН 22-74 - 80 рівні інфразвукового тиску в октавних смугах з середньогеометричними частотами 2, 4, 8 і 16 Гц не повинні перевищувати 105 дБ, а в смузі з частотою 32 Гц-102 дБ. Боротьба з несприятливим впливом інфразвуку повинна вестися в тих же напрямках, що і боротьба з шумом. Найбільш доцільно зменшувати інтенсивність інфразвукових коливань на стадії проектування машин або агрегатів.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі. В безпеці в надзвичайних ситуаціях висвітлено питання ультразвуку та інфразвуку і їх вплив на організ людини.

ВИСНОВКИ

В кваліфікаційній роботі здійснено дослідження процесу організації зонової безпеки комп’ютерної мережі. Основні результати, що отримані після проведеної роботи є наступними:

– здійснено аналіз визначення точок входу в мережу для організації захисту ключових вузлових пристроїв;

– проведено аналіз типового трафіку даних у мережі для виявлення нетипової поведінки та застосування методів та засобів захисту;

– подано аналіз рівневої мережевої безпеки, що дає змогу визначити зони мережевої безпеки;

– досліджено індикатори компроментування комп’ютерної мережі, що уможливлює створення профілю роботи організації для виявлення нетипової поведінки;

– запропоновано використання глибокого тестування мережі для виявлення слабкостей та їх усунення;

– подано основні архітектурні рішення забезпечення захисту мережі на основі зон. У логічній архітектурі узагальнено використання типових підходів організації безпечної роботи мережі. На основі досвіду провідних компаній показано комплексні міри та рішення організації зонової безпеки комп’ютерної мережі. Визначено роль хмарних сервісів в організації безпеки зон для різних сценаріїв;

– запропоновано використання брандмауерів та надано рекомендації щодо впровадження даних засобів для їх ефективної роботи;

– проведено аналіз можливості застосування методів підвищення захисту мереж на основі безпарольної автентифікації, що показує майбутні напрямки розвитку технології для забезпечення зонової безпеки критичних інфраструктур.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі та ультразвуку і інфразвуку, їх вплив на організм людини.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002, ISBN: 978-1-931836-56-2

2. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

3. V. Olifer and N. Olifer, Novye tekhnologii i oborudovanie IP-setei [New technologies and equipment of IP-networks]. St.-Peterburg, Russia: Bhv, 2000, ISBN: 5-8206-0053-3

4. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

5. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 4.04.2022.

6. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

7. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14.04.2022

8. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний

ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 15.04.2022

9. Приїхав до Польщі – користуйся Інтернетом! [Електронний ресурс] – Режим доступу: http://naszwybir.pl/internet/. – Назва з екрану. – Дата звернення: 15.04.2022

10. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

11. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

12. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

13. Cisco Systems Руководство по технологиям объединенных сетей / Cisco Systems - 3-е издание. СПб: “Вильямс”, 2002. – 1040 с.

14. Дебра Литтлджон Шиндер Основы компьютерных сетей / Дебра Литтлджон Шиндер - СПб: "Вильямс", 2002. – 656 с.

15. Коротыгин С. Стандарт IEEE 802.11 и его расширения / С. Коротыгин, А. Нежуренко - Сети и телекоммуникации, вып. 6(25), 2002 г.

16. Марк А. Спортак Компьютерные сети. Книга 1. High-Perfomance Networking. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

17. Марк А. Спортак Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

18. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

19. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

20. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

21. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

22. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

23. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв'язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

24. Френк Г. Сети, связь и потоки / Г. Френк, И. Фриш ; пер. с англ. под ред. Д. А. Поспелова. – Москва : Связь, 1978. – 448 с.

25. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

26. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

27. Шерстнева О. Г. Подходы к оценке качества управления связью / О. Г. Шестернева // Сети и системи связи. – 2008. – №11. – С. 35-41.

28. Стеклов В. К. Проектування телекомунікаційних мереж / В. К. Стеклов, Л. Н. Беркман. ; під ред. В. К. Стеклова – Київ : Техніка, 2002. – 792 с.

29. Кульгин М. Технология корпоративных сетей / М. Кульгин. – Санкт- Петербург : Питер, 1999. – 704 с.

30. Шварц М. Сети связи: протоколы, моделирование и анализ / М. Шварц. – ч.2. – Москва : Наука, 1992. – 272 с.

31. What is SD-WAN (Software-Defined Wide Area Network)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ – Назва з екрану. – Дата звернення: 12.04.2022.

32. SD-WAN vs MPLS: The Pros and Cons of Both Technologies)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/ – Назва з екрану. – Дата звернення: 18.04.2022.

33. Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html?dtid=osscdc000283 – Назва з екрану. – Дата звернення: 18.04.2022.

34. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 20.04.2022.

35. Draft-ietf-nvo3-geneve-08 [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/draft-ietf-nvo3-geneve-08 – Назва з екрану. – Дата звернення: 22.04.2022.

36. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 22.04.2022.

37. Best Network Automation Tools [Електронний ресурс]. – Режим доступу: https://www.dnsstuff.com/network-automation-tools – Назва з екрану. – Дата звернення: 22.04.2022

38. What is network automation? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/automation/network-automation.html – Назва з екрану. – Дата звернення: 23.04.2022.

39. Network automation and orchestration tools review and ratings [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/network-automation – Назва з екрану. – Дата звернення: 23.04.2022.

40. Network automation tools [Електронний ресурс]. – Режим доступу: https://www.pcwdld.com/network-automation-tools-and-software#wbounce-modal – Назва з екрану. – Дата звернення: 23.04.2022.

41. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 23.04.2022.

42. Arregoces, Mauricio, and Maurizio Portolani. Data center fundamentals. Cisco Press, 2003

43. Long, James. Storage Networking Protocol Fundamentals. Pearson Education India, 2006.

44. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

45. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

46. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

47. Membrey, Peter, Eelco Plugge, and David Hows. Practical Load Balancing: Ride the Performance Tiger. Apress, 2012.

48. Odom, Ccie Routing And Switching Exam Certi cation Guide, 4/E. Cisco press, 2004.

49. Kenyon, Tony. Data networks: routing, security, and performance optimization. Digital Press, 2002.

50. R. Froom, B. Sivasubramanian, and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Cisco press.

51. Popovic, Miroslav. Communication protocol engineering. CRC press, 2016. 277

52. J. Appl. Environ. Biol. Sci., 7(3)268-278, 2017

53. S. Tim, Cisco Telepresence Fundamentals. Pearson Education India, 2010.

54. Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization, 2013.

55. Державні будівельні норми України. Інженерне обладнання будинків і споруд. Природне і штучне освітлення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/95.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-28-2006.%20%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%BD%D0%B5%20%D1%96%20%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B5%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

56. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text – Назва з екрану. – Дата звернення: 06.05.2022.

57. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/31562/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_0.00-1.28-10 – Назва з екрану. – Дата звернення: 06.05.2022.

58. Про затвердження Правил охорони праці під час виконання робіт на висоті [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0573-07#Text – Назва з екрану. – Дата звернення: 06.05.2022.

59. Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці та Переліку робіт з підвищеною небезпекою [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0231-05#Text – Назва з екрану. – Дата звернення: 06.05.2022.

60. Проектування електрообладнання об’єктів цивільного призначення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/92.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-23~2010.%20%D0%86%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%BD%D0%B5%20%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B1%D1%83%D0%B4%D0%B8%D0%BD%D0%BA%D1%96%D0%B2%20%D1%96.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

61. Правила улаштування електроустановок [Електронний ресурс]. – Режим доступу: https://art-energetyka.com.ua/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D1%83%D0%BB%D0%B0%D1%88%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-

%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BE%D0%BA.pdf – Назва з екрану. – Дата звернення: 06.05.2022.

62. Про затвердження "Правил будови електроустановок. Електрообладнання спеціальних установок" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0272203-01#Text – Назва з екрану. – Дата звернення: 06.05.2022.

63. Про затвердження державних будівельних норм ДБН В.2.5-56:2010 "Інженерне обладнання будинків і споруд. Системи протипожежного захисту" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0537738-10#Text – Назва з екрану. – Дата звернення: 06.05.2022.

Додатки

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том І

X Міжнародної науково-практичної конференції молодих учених та студентів

24-25 листопада 2021 року

УКРАЇНА
ТЕРНОПІЛЬ – 2021

Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль 24-25 листопада 2021 року

УДК 004.72

М.І. Шоцький, В.В. Федина, С.В. Марценко, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ КЕРУВАННЯ МЕРЕЖЕВИМИ ПРИСТРОЯМИ

M.I.Shotskyi, V.V. Fedyna, S.V. Martsenko, Ph.D., Assoc.

RESEARCH OF PROCESSES OF NETWORK DEVICES CONFIGURATION AUTOMATION

Сучасні мережі змінились у своїх розмірах та складності архітектури. Кількість пристроїв та їх різноманіття приводять до ускладнення процесів налаштування та контролю правильності роботи. Ручне управління стає все більш утрудненим та, у деяких випадках, практично неможливим для мережевого інженера. В таких випадках автоматизація процесів управління та конфігурації мережевими пристроями стає єдиним рішенням для повноцінної та ефективної роботи.

Дослідження процесів автоматизації налаштування та керування мережевими пристроями показує, що є декілька підходів до вирішення цих задач:

- забезпечення налаштування мережевого обладнання через використання бібліотек готових наборів команд для визначених типів обладнання;
- використання графічних інтерфейсів для виконання конфігурування пристроїв;
- здійснення керування пристроями за допомогою стандартизованих протоколів та спеціалізованого програмного забезпечення;
- повна віртуалізація мережевих функцій.

Набори готових командних шаблонів є хорошим підходом у невеликих мережах, де обладнання у більшості своїй однакове. Такий варіант автоматизації дає змогу швидко відновитись у випадку виходу з ладу пристрою за умови наявності аналогічного. Іншим варіантом використання може бути реплікація коду з незначною зміною. До найбільшого недоліку цього методу можна віднести схильність до помилки у коді, оскільки немає функцій перевірки на адекватність налаштування реальній мережі. Уся відповідальність лягає на мережевого фахівця, що ускладнює масштабування цього підходу у великих мережах.

Графічні інтерфейси дають змогу проводити налаштування обладнання для фахівців без необхідності вникнення в архітектуру операційних систем різних виробників і вивчення їх команд. Проте, автоматизація у цьому випадку дуже складна, оскільки вигляд графічних інтерфейсів може змінюватись і написання шаблонних сценаріїв роботи практично неможливе.

Використання стандартизованих протоколів дає змогу проводити налаштування та управління великою кількістю пристроїв, що загалом вирішує задачу автоматизації цих процесів. Проте, більшість програмних продуктів, що забезпечують функціонал керування мережевими вузлами є платними. Реалізація специфічних, для певної мережі, сценаріїв налаштування ускладнене відсутністю доступу до модифікації шаблонів, якщо це не передбачено розробником.

Багато сучасних мереж організовані у гібридному форматі, коли частина ресурсів є фізичними пристроями, а частина віртуальними, що розміщені у хмарі. При такому підході зручним є використання сучасного методу управління інфраструктура як код. Готовими рішеннями які популярні є AWS CoudFormation, Terraform, Ansible, Chef, Puppet, Vagrant, Azure Resource Manager, Google Cloud Resource Manager, Serverless Framework. Програмування є невід'ємною частиною їх роботи.

Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль 24-25 листопада 2021 року

УДК 004.72

М.І. Шоцький, В.В. Федина
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСУ ОРГАНІЗАЦІЇ ЗОНОВОЇ БЕЗПЕКИ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

M.I.Shotskyi, V.V. Fedyna

RESEARCH OF THE PROCESS OF ZONE SECURITY ORGANIZATION IN A COMPUTER NETWORK

Захист інформації та інформаційних ресурсів набуває все більш вагомого значення при проектуванні нових мереж та модернізації роботи існуючих. Таким чином, актуальною задачею є дослідження організації зонової безпеки для ефективної та безпечної роботи мереж різного призначення. При дослідженні проектування безпеки в мережах потрібно враховувати низку факторів, що визначають особливості роботи організації, наборів обладнання та потоків трафіку, що мають бути захищені.

Аналіз літературних джерел дав змогу сформувати ряд задач, що потребують вирішення при організації зонової безпеки, а саме:

- дослідити розмір мережі для визначення правильного підходу до організації мережевої безпеки;
- визначити набори обладнання, їх тип та можливості для впровадження спроектованих рішень;
- провести аналіз потоків даних з визначенням рівнів важливості для забезпечення роботи організації;
- провести зонування мережі з використанням зон безпеки другого рівня, третього рівня або їх поєднання.

Дослідження розмірів мережі дасть змогу визначити чи створення зональної безпеки не буде приводити до ускладнення її роботи та подальшого обслуговування адмініструючим персоналом. В маленьких мережах, в багатьох випадках, достатнім рішенням є використання списків контролю доступу для організації контролю трафіку. При невеликих кількостях типів потоків даних процес написання таких списків не потребує особливих затрат часу та в подальшому спрощує керування мережею при зміні адміністратора. У мережах з динамічними потоками даних такий підхід працювати не буде або його робота буде неефективною.

Аналіз наборів обладнання дасть змогу провести аудит мережевих ресурсів з визначенням версій операційних систем, апаратних можливостей нести додаткові навантаження щодо аналізу потоків даних, сумісності різного обладнання між собою при розгортанні єдиної політики безпеки мережі.

Для різних мереж не всі потоки даних є однаковими. Створення правильної політики безпеки мережевих ресурсів організації вимагає чіткого розуміння точок входу та виходу трафіку, переходів трафіку між різними сегментами мережі, класифікації наборів даних та ін. Створення зональної безпеки базується на створенні правил роботи з даними чітко визначеними у політиці безпеки мережі організації.

Створення зонування потребує визначення на яких рівнях у мережі буде застосовуватись дана технологія. Використання зон безпеки другого рівня буде акцентувати увагу на інтерфейсах другого рівня і включатиме списки інтерфейсів в зоні, активні політики безпеки, що будуть застосовувати правила до трафіку який проходитиме через інтерфейс. Зональна безпека, що базується на третьому рівні використовує для організації інтерфейси третього рівня.