Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ

завідувач кафедри

мережевих та інтернет технологій

_____ Юрій КРАВЧЕНКО

«___»_____2023 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»

за спеціальністю 172 «Телекомунікації та радіотехніка»

освітньо-професійна програма «Мережеві та інтернет технології»

на тему:

Розробка рекомендацій щодо впровадження комплексної безпеки в корпоративній мережі

Виконав: студент групи МІТ-41

Михайло Федорук _____

Керівник: асистент кафедри мережевих та інтернет технологій

к.т.н., асистент Олена СТАРКОВА

_____

Київ 2023

ЗАВДАННЯ НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Федоруку Михайлу Богдановичу

(прізвище, ім'я, по батькові)

1. Тема роботи:

Розробка рекомендацій щодо впровадження комплексної безпеки в корпоративній мережі

затверджена на засіданні кафедри МІТ «07» грудня 2022 р. протокол №5

2. Термін здачі закінченої роботи «31» травня 2023 р.

3. Вихідні дані до проекту (роботи)

Сучасні технології інформаційної безпеки

4. Зміст пояснювальної записки

Вступ

1. Теоретичні основи інформаційної безпеки

2. Сучасні корпоративні мережі

3. Комплексна безпека у сучасних корпоративних мережах

4. Розробка рекомендацій щодо впровадження комплексної безпеки в корпоративну мережу

5. Впровадження базових рекомендацій по налаштуванню безпеки мережі на прикладі симуляції Packet tracer

5. Перелік графічного матеріалу 8-10 слайдів

Дата видачі завдання

Керівник роботи к.т.н., асистент Олена СТАРКОВА

(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання

М.Б. Федорук

(підпис)

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	20.01.2023	
2	Розділ 1	15.02.2023	
3	Розділ 2	15.03.2023	
4	Розділ 3	20.04.2023	
5	Доповідь та слайди	25.05.2023	
6	Пояснювальна записка	31.05.2023	

Здобувач вищої освіти _____ Михайло ФЕДОРУК

(підпис)

Керівник _____ Олена СТАРКОВА

(підпис)

РЕФЕРАТ

Дипломний проект: 90 сторінок, 6 рисунки, 12 джерел.

Дипломна робота спрямована на проведення аналізу та дослідження існуючих системи захисту інформації, зокрема оцінку технічних та програмних засобів безпеки. Основна мета полягає в розробці рекомендацій з поліпшення цієї системи для забезпечення вищого рівня безпеки підприємства.

Об'єктом дослідження є методи, моделі та інструменти, які використовуються для створення комплексних систем захисту інформації.

Методи дослідження включають аналіз, синтез та моделювання для глибшого розуміння та вивчення досліджуваної проблеми.

Наукова унікальність роботи полягає у вивченні найбільш сучасних тенденцій безпеки та глибокому детальному підході до розробки рекомендацій щодо впровадження комплексної безпеки в корпоративній мережі. Цей підхід має потенціал створити значний прогрес у сфері безпеки та забезпечити високу надійність корпоративних інформаційних ресурсів.

Практичне значення роботи полягає в дослідженні і аналізі найновітніших загроз що сприятиме впровадженню комплексної безпеки для організацій, що оперують корпоративними мережами. Це дослідження спрямоване на пошук новаторських підходів до забезпечення комплексної безпеки інформації в корпоративних мережах.

ABSTRACT

Diploma Project: 90 pages, 6 figures, 12 references.

The diploma thesis aims to analyze and investigate existing information security systems, particularly evaluating technical and software security measures. The main objective is to develop recommendations for enhancing this system to achieve a higher level of security for the enterprise.

The research focuses on the methods, models, and tools used in creating comprehensive information security systems.

The research methods include analysis, synthesis, and modeling to gain a deeper understanding and explore the research problem.

The scientific novelty of the work lies in studying the most current security trends and taking a detailed approach to developing recommendations for implementing comprehensive security in corporate networks.

This approach has the potential to make significant progress in the field of security and ensure the high reliability of corporate information resources.

The practical significance of the work lies in the research and analysis of the latest threats, which will contribute to the implementation of comprehensive security measures for organizations operating corporate networks. This research aims to explore innovative approaches to ensuring information security in corporate networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SSH — мережевий протокол рівня застосунків

ІКСМ - інформаційно-комунікаційні системи та мережі

ПК - персональний комп'ютер

ОС - операційна система

МЕ - міжмережевий екран

ТРМ - територіально розподілена мережа

ASA - Adaptive Security Appliance

FTP - протокол передачі файлів

АРМ - автоматизоване робоче місце

ЛОМ - локальна обчислювальна мережа

ІТС - інформаційно-телекомунікаційна система

DHCP - протокол динамічної конфігурації хоста

СУБД - система управління базами даних

IP - протокол інтернету

АС - автоматизована система

АСУ - автоматизована система управління

ІБ - інформаційна безпека

MAC - контроль доступу до медіа

БД - база даних

ЕОМ - електронно обчислювальна машина

АРМ - автоматизоване робоче місце

ПЕОМ - персональна електронна обчислювальна машина

ПЗ - програмне забезпечення

IP - протокол інтернету

ІС - інформаційна система

VLAN - віртуальна локальна область мережі

ВСТУП

В сучасному світі, де інформаційні технології стають невід'ємною частиною практично всіх аспектів підприємницької діяльності, забезпечення безпеки корпоративної мережі стає вельми актуальною задачею. Комплексна безпека в корпоративній мережі стає важливим аспектом забезпечення надійності, конфіденційності та цілісності інформації, а також захисту від зовнішніх загроз.

Ділова активність організацій, використання електронних засобів комунікації та передачі даних, а також збільшення обсягу цифрової інформації ставлять перед компаніями важливе завдання - забезпечити безпеку корпоративної мережі. Порушення безпеки мережі може мати серйозні наслідки, такі як втрата даних, виток конфіденційної інформації, пошкодження репутації компанії та значні фінансові збитки.

Однак, багато організацій часто знаходяться перед складністю вибору ефективних методів і стратегій забезпечення безпеки своєї мережі. Задача розробки та впровадження комплексних рекомендацій з безпеки в корпоративній мережі стає важливою для забезпечення безпеки і надійності діяльності організації.

Метою даної дипломної роботи є розробка рекомендацій щодо впровадження комплексної безпеки в корпоративній мережі з метою забезпечення конфіденційності, цілісності та доступності інформації, а також захисту від внутрішніх та зовнішніх загроз. Виконання даної роботи дозволить виявити потенційні ризики безпеки мережі, проаналізувати існуючі методи та інструменти захисту і розробити рекомендації щодо їх впровадження.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Проаналізувати основні загрози та вразливості, з якими стикаються корпоративні мережі.
2. Вивчити сучасні підходи та методики безпеки мереж та їх ефективність.

3. Виявити основні складові комплексної безпеки, необхідні для корпоративних мереж.
4. Розробити стратегію комплексної безпеки, враховуючи особливості конкретної організації.
5. Впровадити запропоновані рекомендації в корпоративній мережі та оцінити їх ефективність.

Об'єктом дослідження даної дипломної роботи є корпоративні мережі, які використовуються в організаціях для обміну даними та забезпечення роботи бізнес-процесів. Корпоративна мережа є комплексною системою, що включає різноманітні пристрої, програмне забезпечення, комунікаційні канали та інфраструктуру, які забезпечують передачу, зберігання та обробку даних в організації.

Предметом дослідження є розробка рекомендацій щодо впровадження комплексної безпеки в корпоративні мережі. Комплексна безпека включає в себе широкий спектр аспектів, пов'язаних із забезпеченням цілісності, конфіденційності, доступності та автентичності даних, а також захисту від несанкціонованого доступу, вразливостей та загроз безпеці.

Дослідження включатиме аналіз основних загроз та вразливостей, з якими стикаються корпоративні мережі, вивчення сучасних підходів та методик безпеки мереж, виявлення основних складових комплексної безпеки, розробку стратегії комплексної безпеки, впровадження рекомендацій та оцінку їх ефективності. Результати дослідження матимуть практичне значення для організацій, оскільки дозволять покращити безпеку та надійність їх корпоративних мереж, зменшити ризики кібератак та забезпечити безпечне функціонування бізнес-процесів.

Методологія що визначає основні кроки та інструменти, які використовуються в рамках даної дипломної роботи:

1. Аналіз наукової літератури: Здійснюється систематичний аналіз наукової літератури, наявних досліджень, публікацій та статей, що

стосуються безпеки корпоративних мереж. Цей аналіз допомагає усвідомити сучасний стан досліджень у галузі та визначити актуальні проблеми та тенденції.

2. Збір та аналіз статистичних даних: Проводиться збір та аналіз статистичних даних про кібератаки, вразливості мереж, витрати на безпеку та інші аспекти безпеки корпоративних мереж. Ці дані допомагають виявити основні загрози та вразливості, що можуть бути використані при розробці рекомендацій.

3. Дослідження практичних випадків: Вивчаються практичні випадки впровадження безпеки в корпоративні мережі. Це можуть бути дослідження конкретних організацій, які впроваджували стратегії та методи безпеки, або аналіз недавніх кібератак та заходів, прийнятих для їх запобігання та реагування. Це дозволяє здобути практичні уроки та визначити ефективні підходи до безпеки мереж.

4. Розробка рекомендацій та стратегії безпеки: На основі отриманих даних, аналізу та експертних оцінок розробляються рекомендації та стратегія безпеки для впровадження в корпоративну мережу. Рекомендації можуть стосуватися технічних заходів безпеки, політик безпеки, процедур управління безпекою та навчання персоналу.

5. Оцінка ефективності рекомендацій: Проводиться оцінка ефективності впроваджених рекомендацій та стратегії безпеки. Це може включати оцінку зменшення загроз та вразливостей, покращення надійності мережі та забезпечення безпеки даних.

Використання цієї методології дослідження дозволить здійснити комплексний аналіз проблеми впровадження комплексної безпеки в корпоративній мережі та розробити конкретні рекомендації, що сприятимуть покращенню безпеки, надійності та стійкості мережі.

Дана дипломна робота відзначається своєю **науковою новизною**, оскільки пропонує оригінальний підхід до розробки рекомендацій щодо впровадження

комплексної безпеки в корпоративній мережі. Нижче наведено основні аспекти, які визначають наукову новизну даної роботи:

1. Комплексний підхід до безпеки мереж: У даній роботі використовується комплексний підхід до безпеки корпоративної мережі, що охоплює не лише технічні аспекти, а й аспекти управління безпекою, навчання персоналу та політики безпеки. Цей підхід сприяє створенню інтегрованої системи безпеки, яка забезпечує високий рівень захисту мережі від різних загроз та вразливостей.
2. Аналіз сучасних тенденцій: Робота включає аналіз сучасних тенденцій у галузі безпеки мереж, враховуючи нові загрози та вразливості, які виникають у зв'язку з розвитком технологій та кіберзлочинності. Це дозволяє враховувати актуальність розроблених рекомендацій та забезпечувати адаптивність до змінних умов.
3. Практична спрямованість: Дана робота має сильну практичну спрямованість, оскільки розроблені рекомендації та стратегії безпеки базуються на аналізі практичних випадків та експертних оцінках. Це дозволяє забезпечити високу релевантність та застосовність результатів дослідження у реальних умовах.
4. Значення для організацій: Результати даної роботи матимуть практичне значення для організацій, які прагнуть забезпечити безпеку своїх корпоративних мереж. Рекомендації та стратегії безпеки, розроблені у роботі, допоможуть покращити безпеку, зменшити ризики кібератак та забезпечити безпечне функціонування бізнес-процесів.

Таким чином, дана дипломна робота має наукову новизну, оскільки пропонує комплексний підхід до безпеки корпоративних мереж, враховує сучасні тенденції, має практичну спрямованість та високу значущість для організацій.

Виконання даної дипломної роботи є **актуальним**, оскільки забезпечення безпеки корпоративної мережі стає першочерговим завданням для багатьох

компаній. Результати дослідження та розроблені рекомендації сприятимуть підвищенню рівня безпеки та надійності мережі, а також зниженню ризику виникнення інформаційних загроз.

У подальших розділах дипломної роботи будуть детально розглянуті аналіз існуючих методів та інструментів забезпечення безпеки мережі, а також розробка та впровадження комплексних рекомендацій. Завершення дослідження і виконання поставлених завдань сприятимуть створенню надійного, захищеного та стійкого середовища для обміну інформацією в корпоративній мережі.

Таким чином, дана дипломна робота відповідає актуальним потребам сучасного бізнесу та інформаційних технологій, а результати її виконання можуть бути використані для покращення безпеки корпоративних мереж та захисту цінної інформації.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комплексна безпека в корпоративній мережі є складним процесом, що вимагає розуміння різних теоретичних аспектів безпеки та їх впливу на захист мережевої інфраструктури. Далі наведено ключові теоретичні аспекти, які необхідно розглянути при розробці рекомендацій щодо впровадження комплексної безпеки.

1.1 Сучасні загрози та ризики безпеки

Загрози та ризики безпеки є невід'ємною частиною комплексної безпеки корпоративної мережі. Детальне розглядання різноманітних типів загроз та оцінка ризиків допомагає розробити ефективну стратегію безпеки та прийняти необхідні заходи для запобігання і зменшення потенційних проблем.

1.1.1 Кібератаки

Хакерські атаки є одним з найпоширеніших видів кіберзагроз, що становлять серйозну загрозу для корпоративних мереж. Ці атаки здатні завдати значних збитків, порушити конфіденційність інформації, а також поставити під загрозу репутацію та фінансову стабільність організації. Хакерські атаки зазвичай проводяться шляхом використання різноманітних методів та технік, таких як експлуатація слабких паролів, експлуатація вразливостей програмного забезпечення, атаки на мережеві протоколи тощо.

Одним з найбільш поширених методів хакерських атак є експлуатація слабких паролів. Багато користувачів вибирають прості та легко запам'ятовувані паролі, які швидко можуть бути підібрані шляхом перебору або використання атак, що ґрунтуються на словнику. Зловмисники також можуть використовувати соціальний інжиніринг, щоб отримати доступ до паролів користувачів,

наприклад, шляхом використання підроблених веб-сторінок або фішингових електронних листів.

Окрім атак на паролі ще одним видом хакерських атак є експлуатація вразливостей програмного забезпечення. Комп'ютерні програми і операційні системи часто мають певні слабкі місця, які можуть бути використані зловмисниками для незаконного доступу до системи або виконання шкідливого коду. Ці вразливості можуть бути результатом програмних помилок, недостатньої перевірки вхідних даних або недостатнього оновлення програмного забезпечення. Зловмисники активно використовують ці вразливості, щоб отримати несанкціонований доступ до системи, викрасти конфіденційні дані або пошкодити систему.

Атаки на мережеві протоколи також є поширеним методом хакерських атак. Зловмисники можуть використовувати різноманітні техніки, такі як перехоплення пакетів, аналіз мережевого трафіку та зловживання протоколами для отримання несанкціонованого доступу до мережі або отримання конфіденційної інформації. Це може призвести до розкриття конфіденційних даних, перехоплення аутентифікаційних даних або впровадження шкідливого коду в мережу.

Крім хакерських атак, варто відзначити інші види кібератак, такі як фішинг, використання вразливостей програмного забезпечення, деніал-оф-сервіс (DoS) та деніал-оф-сервіс-атаки (DDoS), викрадення облікових записів та інші. Кожен з цих видів атак має свої характеристики та потенційні наслідки, які необхідно враховувати при розробці стратегій комплексної безпеки.

Статистика та дослідження підтверджують поширеність кібератак та їх вплив на корпоративні мережі. Зокрема, згідно з Verizon 2021 Data Breach Investigations Report, 85% усіх кібератак відбуваються за рахунок використання низько складних атак та використання слабких паролів. Дослідження Cybersecurity Ventures показують, що до 2023 року прогнозується зростання витрат на відновлення внаслідок кібератак до $10,5 трильйонів. Особливо

тривожним є зростання фішингових атак, де за даними APWG (Anti-Phishing Working Group), виявлено понад 100 мільйонів нових фішингових електронних листів, пов'язаних з викраденням облікових записів.

Ці статистичні дані та дослідження підкреслюють важливість розуміння загроз кібербезпеці та розробку ефективної стратегії комплексної безпеки. Забезпечення надійного захисту від кібератак вимагає використання заходів, таких як підвищення свідомості співробітників, використання сучасних антивірусних програм та мережевих рішень, постійний моніторинг та аналіз загроз, а також регулярне оновлення систем та програмного забезпечення. Тільки шляхом глибокого розуміння кібератак та їх наслідків можна розробити ефективні заходи для захисту корпоративних мереж від цих загроз.

1.1.2 Витоки даних

Витоки даних є однією з найбільш серйозних загроз для сучасного цифрового світу. Вони можуть призвести до незаконного розголошення конфіденційної інформації, такої як особисті дані, комерційні та бізнес-інформація, банківські реквізити, а також інші конфіденційні дані, які можуть завдати значної шкоди як організаціям, так і їхнім клієнтам.

Одним з основних джерел витоків даних є внутрішній фактор. Це означає, що самі працівники організації, свідомо або несвідомо, викривають конфіденційну інформацію. Внутрішній фактор може включати недобросовісних співробітників, які мають доступ до конфіденційних даних і зловживають своїми привілеями для особистої користі або з метою завдання шкоди організації. Також можуть мати місце ненавмисні витоки даних через недбалість, помилки або недостатню охорону інформації з боку працівників. За даними досліджень Ponemon Institute, внутрішній фактор є причиною більш ніж половини витоків даних (51%).

Зовнішні атаки є ще одним значним джерелом витоків даних. Це означає, що зловмисники, які знаходяться поза організацією, використовують різноманітні методи та техніки для незаконного доступу до інформації. Ці атаки можуть включати хакерські атаки, фішинг, використання вразливостей програмного забезпечення та інші техніки, спрямовані на отримання незаконного доступу до системи або мережі. Це може призвести до крадіжки конфіденційних даних, витоку комерційної та бізнес-інформації, а також до розголошення особистих даних клієнтів. За даними Verizon Data Breach Investigations Report 2021, зовнішні атаки стоять за 70% всіх кібер інцидентів.

Недостатня безпека мережі та систем також може бути причиною витоків даних. Це може включати використання застарілих або неправильно налаштованих захисних механізмів, відсутність регулярних оновлень та патчів, недостатній контроль доступу до конфіденційної інформації та інші проблеми, що можуть бути використані зловмисниками для незаконного доступу. Недостатня безпека може також включати відсутність хорошого шифрування даних, слабкі паролі, недостатній моніторинг мережі та системи. За даними дослідження Verizon Data Breach Investigations Report 2021, 61% всіх кібер інцидентів були пов'язані з недостатньою безпекою мережі та систем організації.

Крім того, втрати або крадіжки пристроїв можуть також стати причиною витоків даних. Це може включати втрату чи крадіжку ноутбуків, смартфонів, зовнішніх носіїв даних, які містять конфіденційну інформацію. В таких випадках, зловмисник, який отримує фізичний доступ до пристрою, може отримати доступ до конфіденційних даних, які зберігаються на ньому. Втрати або крадіжки пристроїв є однією з найпоширеніших причин витоків даних, особливо у випадку мобільних пристроїв.

Підсумкова статистика:

- За даними дослідження Ponemon Institute, внутрішній фактор є причиною більш ніж половини витоків даних (51%).

- Згідно з Verizon Data Breach Investigations Report 2021, зовнішні атаки відіграли роль у 70% всіх кібер інцидентів у 2020 році.
- За даними того ж звіту, 61% всіх кібер інцидентів були пов'язані з недостатньою безпекою мережі та систем організації.
- За даними звіту "IBM Cost of Data Breach Report 2021", середня вартість витоку даних у світі склала 4,24 мільйона доларів, а середня кількість днів для виявлення та зупинки витоку становила 287 днів.
- За даними "Identity Theft Resource Center" (ITRC), у 2020 році було зафіксовано 1 108 випадків витоку даних у Сполучених Штатах Америки, що призвело до компрометації понад 300 мільйонів записів особистих даних.
- Згідно зі звітом "Data Breach Investigations Report 2021" від Verizon, найбільш поширеними типами витоків даних є крадіжка акаунтів (61%), фішинг (36%), злам систем (29%) та зловживання привілеями (19%).

Ці статистичні дані підкреслюють серйозність проблеми витоків даних і показують, що вони є глобальною проблемою, яка має значний економічний вплив на організації та суспільство. Вони можуть призвести до значних фінансових втрат, порушення довіри клієнтів та пошкодження репутації компанії.

1.1.3 Внутрішні загрози

Внутрішні загрози є серйозними факторами, які сприяють витоку даних та порушенню безпеки в корпоративній мережі. Ці загрози походять від осіб, які мають прямий доступ до систем та ресурсів організації, включаючи співробітників, підрядних працівників та стажерів.

Недосконаліть внутрішніх процесів та політик безпеки: Один з основних факторів, які створюють внутрішні загрози, - це недосконаліть внутрішніх процесів та політик безпеки. Недостатньо чіткі правила щодо контролю доступу,

слабка політика паролів, відсутність відповідальності за безпеку даних - все це може сприяти зловживанню привілеїв та небажаним діям з боку працівників.

1.1.4 Соціальна інженерія

Соціальний інжиніринг є одним з найбільш складних та небезпечних видів загроз. Цей метод атаки базується на маніпулюванні людьми, заманюючи їх у розголошення конфіденційної інформації, виконання шкідливих дій або встановлення шкідливого програмного забезпечення.

Соціальний інжиніринг є процесом отримання конфіденційної інформації шляхом маніпулювання та обману людей, заманюючи їх до розголошення цієї інформації або виконання небезпечних дій. Соціальні інженери використовують психологічні методи та соціальні навички для отримання доступу до систем, даних або ресурсів, на які вони не мають легального доступу.

Соціальний інжиніринг може включати в себе фішинг, фальшиві дзвінки, підроблення особистості, викрадення даних та багато інших методів. Головна мета соціального інжинірингу - використати людську довіру, небажання сприймати небезпеку та використовувати ці слабкості для досягнення своїх злочинних цілей.

Соціальний інжиніринг становить серйозний виклик для організацій та індивідуальних користувачів, оскільки він атакує найслабшу ланку в кібербезпеці - людей. Основні виклики, пов'язаних з соціальним інжинірингом, включають наступне:

1. Людська природа та психологія: Соціальний інжиніринг ефективний через використання людських слабкостей, таких як довіра, небажання сприймати небезпеку, соціальна інертність та бажання допомогти іншим. Люди часто несвідомо розголошують конфіденційну інформацію або виконують небезпечні дії, вважаючи, що вони спілкуються з надійною особою або діють на благо організації.

2. Технологічний прогрес: З розвитком технологій соціальний інжиніринг стає все складнішим та субтильнішим. Зловмисники використовують різноманітні канали комунікації, такі як електронна пошта, соціальні мережі, мобільні додатки тощо, щоб наблизитися до своїх жертв. Вони можуть виглядати дуже переконливо та використовувати широкий спектр технік, щоб зламати бар'єри безпеки.

3. Низький рівень освіченості: Багато людей не мають достатньої освіти та усвідомлення про соціальний інжиніринг та його наслідки. Вони можуть бути недостатньо підготовлені до виявлення ознак маніпуляцій та шахрайства, що робить їх вразливими перед атаками.

4. Загроза зсередини: Соціальний інжиніринг може бути особливо небезпечним, оскільки він може бути проведений всередині самої організації. Зловмисники можуть використовувати внутрішніх співробітників, щоб отримати доступ до конфіденційної інформації або виконати шкідливі дії.

5. Соціальні мережі: Зараз соціальні мережі стали важливим комунікаційним засобом для багатьох людей. Однак, вони також стали потужним інструментом для соціального інжинірингу. Зловмисники можуть отримувати доступ до профілів людей, збирати персональну інформацію та використовувати її для маніпуляцій та атак.

Соціальний інжиніринг створює безліч загроз, які можуть мати серйозні наслідки для організацій та індивідуальних користувачів. Деякі з найпоширеніших загроз, пов'язаних з соціальним інжинірингом, включають:

1. Виток конфіденційної інформації: За допомогою соціального інжинірингу, зловмисники можуть отримати доступ до конфіденційної інформації, такої як паролі, номери соціального страхування, фінансові дані тощо. Ця інформація може бути використана для крадіжки ідентичності, фінансових шахрайств або шкоди бізнесу.

2. Вторгнення в інформаційну систему: За допомогою соціального інжинірингу зловмисники можуть отримати доступ до комп'ютерних систем і мереж. Вони можуть виконати вторгнення, встановити шкідливе програмне забезпечення, викрасти дані або навіть зруйнувати систему. Це може призвести до великих фінансових втрат та порушення діяльності організацій.

3. Фінансові шахрайства: Соціальний інжиніринг також може використовуватися для виконання фінансових шахрайств. Зловмисники можуть зламати акаунти користувачів, використовувати крадену ідентичність для здійснення фінансових операцій або шахрайських актів. Це може призвести до втрати грошей та психологічних наслідків для жертв.

4. Крадіжка ідентичності: Соціальний інжиніринг може бути використаний для крадіжки ідентичності, що може мати серйозні наслідки для особистих фінансів, репутації та безпеки жертви. Зловмисники можуть використовувати отриману конфіденційну інформацію для відкриття фальшивих акаунтів, оформлення кредитів на ім'я жертви або виконання інших злочинних дій.

5. Соціальні наслідки: Від соціального інжинірингу страждають не тільки організації та індивідуальні користувачі, але й суспільство в цілому. Зловмисники можуть використовувати отриману інформацію для поширення дезінформації, маніпулювання громадською думкою або виконувати політичні чи соціальні акти насильства.

Соціальний інжиніринг є серйозною загрозою для організацій та індивідуальних користувачів. Його складність та субтильність створюють потенційно небезпечне середовище, в якому зловмисники можуть використовувати людські слабкості для отримання незаконного доступу до інформації та здійснення шкідливих дій. Однак, за допомогою правильних

заходів безпеки, свідомості та освіченості, можна знизити ризик і виявити спроби соціального інжинірингу.

Захист від соціального інжинірингу вимагає постійного вдосконалення та зусиль з боку організацій та індивідуальних користувачів. Тільки шляхом поєднання технологічних рішень, освіченості та правильних практик ми можемо забезпечити надійний захист від соціального інжинірингу та зберегти конфіденційність, безпеку та добробут наших організацій та особистих життів.

1.2 Комплексний підхід до безпеки

Комплексний підхід використовується найкраще у контексті комплексності загроз, з якими стикаються корпоративні мережі. Кіберзагрози постійно еволюціонують і стають все більш складними та високотехнологічними. Хакери, зловмисники та інші злочинці намагаються використовувати різноманітні техніки, щоб отримати несанкціонований доступ до систем, викрасти конфіденційну інформацію, завдати фінансової шкоди або зашкодити репутації компанії.

Використання комплексного підходу відображає реальну природу загроз та вимагає всебічного розгляду різних вимірів безпеки.

Комплексний підхід дозволяє оцінити всі можливі ризики та вразливості системи, а не обмежуватися окремими аспектами безпеки. Він охоплює технічні, організаційні та процесні аспекти безпеки. Шляхом ідентифікації потенційних ризиків та прийняття відповідних заходів забезпечується передбаченість та вчасна реакція на загрози.

Комплексний підхід включає в себе різноманітні заходи безпеки, такі як розробка імунітету до кібератак, регулярне оновлення програмного забезпечення та апаратури, навчання персоналу щодо кібербезпеки, резервне копіювання даних та планування відновлення після інциденту. Він сприяє взаємодії різних

відділів організації, включаючи IT, керівництво, відділ безпеки та персонал, що допомагає впроваджувати стратегії безпеки як цілісну систему.
Комплексна безпека забезпечує гнучкість і адаптивність до змін у загрозах та технологічному середовищі. Це дозволяє організації ефективно реагувати на нові виклики та швидко адаптуватися до змін.

Такий підхід до безпеки в корпоративних мережах є необхідною складовою для забезпечення надійного захисту інформації та ресурсів компанії. Цей підхід передбачає використання цілісної системи заходів, яка охоплює всі аспекти безпеки, включаючи технічні, організаційні та людські аспекти. Основна унікальність комплексного підходу полягає у тому, що він поєднує різноманітні методи, технології та стратегії для створення цілісного безпечного середовища.

Одна з головних особливостей комплексного підходу полягає в тому, що він охоплює весь життєвий цикл корпоративної мережі - від проектування та розгортання до експлуатації та підтримки. Це означає, що безпека враховується на всіх етапах розвитку мережі, що дозволяє ефективно виявляти, запобігати та вирішувати потенційні проблеми безпеки.

Ще однією важливою особливістю комплексного підходу є інтеграція різноманітних заходів безпеки. Він поєднує технічні рішення, такі як фаєрволи, системи виявлення і запобігання вторгнень, шифрування даних, з організаційними політиками, процедурами та навчанням персоналу. Це дозволяє створити повністю функціональну систему безпеки, яка враховує як технічні аспекти, так і людський фактор, який часто є слабким місцем в системах безпеки.

Комплексний підхід також передбачає постійне моніторинг і оновлення системи безпеки. Він вимагає систематичної оцінки загроз, ідентифікації нових вразливостей та впровадження відповідних заходів для їх запобігання. Це включає в себе регулярне оновлення програмного забезпечення, аналіз журналів подій, аудит безпеки та проведення інших заходів для забезпечення безпеки на всіх рівнях.

Комплексний підхід до безпеки в корпоративних мережах є надійним і ефективним способом забезпечити конфіденційність, цілісність та доступність даних, а також захистити важливі ресурси компанії від зовнішніх загроз. Його унікальність полягає в комплексному підході, який об'єднує технології, політики, процедури та навчання персоналу для створення надійної безпечної інфраструктури. Застосування комплексного підходу дозволяє підвищити рівень безпеки корпоративних мереж і зменшити ризики, пов'язані з витоком чутливої інформації, зламом системи або втратою доступу до ресурсів.

Загалом, комплексний підхід до безпеки в корпоративних мережах є ключовим елементом успішного захисту компанії від сучасних загроз. Його унікальність полягає в інтеграції технологій, політик, процедур та навчання персоналу для створення цілісної системи безпеки. Застосування комплексного підходу дозволяє компаніям забезпечити надійний захист своїх даних, ресурсів та інфраструктури, а також відповідати вимогам сучасного безпечного бізнес-середовища.

РОЗДІЛ 2. СУЧАСНІ КОРПОРАТИВНІ МЕРЕЖІ

У сучасному бізнес-середовищі корпоративні мережі відіграють важливу роль у забезпеченні ефективної комунікації, обміну даними та забезпеченні безпеки інформації. Цей розділ присвячений розгляду концепції сучасних корпоративних мереж, їх складових елементів та різновидів.

2.1 Концепція корпоративної мережі

Корпоративна мережа - це інфраструктура, що об'єднує різні комп'ютери, пристрої та сервери в межах організації з метою забезпечення обміну даними, спільного доступу до ресурсів та комунікації між співробітниками. Вона побудована на основі комп'ютерних мереж і використовує різні технології та протоколи для забезпечення функціональності та безпеки.

Сучасні корпоративні мережі є невід'ємною складовою успішного функціонування сучасних організацій. Вони стали незамінними інструментами для обміну даними, спільної роботи, комунікації та забезпечення безпеки і ефективності роботи бізнесу. У зв'язку з постійними змінами в технологіях, вимогами до безпеки і зростанням обсягів даних, сучасні корпоративні мережі стають все складнішими і потребують комплексного підходу до проектування, розгортання і управління.

Однією з основних характеристик сучасних корпоративних мереж є їх висока швидкість передачі даних. Широкосмуговий доступ до мережі, використання оптоволоконних кабелів і бездротових технологій дозволяють організаціям передавати великі обсяги даних між різними підрозділами та віддаленими локаціями миттєво. Це забезпечує швидку обробку і обмін інформацією, що в свою чергу підвищує продуктивність та ефективність роботи співробітників.

Іншою важливою особливістю сучасних корпоративних мереж є їх масштабованість. Організації можуть розширювати свої мережі залежно від зростання бізнесу і потреб, додаючи нові вузли, підрозділи та підключаючи додаткові користувачів. Це дозволяє адаптувати мережу до змінних вимог і зберігати її працездатність навіть при швидкому розширенні організації.

Однак, зростання складності мережі призводить до зростання загроз безпеці інформації.

2.2 Складові елементи корпоративної мережі

2.2.1 Комутатори

Комутатори є основними складовими елементами корпоративної мережі. Вони забезпечують локальне з'єднання між комп'ютерами та пристроями в мережі. Комутатори дозволяють передавати дані лише тим пристроям, які є їх призначеними отримувачами, що робить мережу більш ефективною і безпечною.

Рисунок 2.2.1 – Комутатор

2.2.2 Маршрутизатори

Маршрутизатори відповідають за передачу даних між різними мережами. Вони приймають пакети даних і приймають рішення про найкращий шлях для їх доставки. Маршрутизатори забезпечують комунікацію між локальною мережею і зовнішніми мережами, такими як Інтернет.

Рисунок 2.2.2 – Маршрутизатор

2.2.3 Сервери

Сервери є центральними вузлами корпоративної мережі і надають різні сервіси та ресурси для користувачів. Наприклад, файлові сервери забезпечують спільний доступ до файлів, сервери електронної пошти обробляють та доставляють електронну пошту, а сервери баз даних зберігають та керують корпоративною інформацією.

2.2.4 Клієнти

Клієнт є однією з важливих складових корпоративних мереж, яка відіграє ключову роль у забезпеченні зв'язку між користувачами та різноманітними ресурсами в мережевому середовищі організації. Клієнт - це будь-який пристрій або програмне забезпечення, що отримує доступ до корпоративної мережі з метою виконання різних завдань, спілкування та отримання необхідної інформації.

Клієнти в корпоративних мережах можуть бути фізичними пристроями, такими як комп'ютери, ноутбуки, планшети, смартфони, або ж програмними рішеннями, такими як веб-браузери, електронна пошта, месенджери та інші додатки. Вони забезпечують доступ користувачам до мережевих ресурсів, таких як файли, бази даних, додатки, принтери та інші послуги, що надаються в мережі.

Одна з ключових вимог до клієнтів в корпоративних мережах - це безпека. Клієнти повинні мати механізми захисту, такі як аутентифікація, авторизація та шифрування, щоб забезпечити конфіденційність, цілісність і доступність інформації. Вони також повинні відповідати політикам безпеки організації, що може включати встановлення паролів, використання мережевих сертифікатів та контроль доступу до ресурсів.

Клієнти можуть використовувати різні протоколи комунікації, такі як TCP/IP, HTTP, FTP, SMTP, POP3 тощо, для взаємодії з мережевими ресурсами. Це дозволяє їм передавати дані, отримувати відповіді та взаємодіяти з різними службами, що працюють в мережі.

2.2.5. Проводова та безпроводова інфраструктура

Корпоративна мережа може використовувати проводову (Ethernet) та безпроводову (Wi-Fi) інфраструктуру для забезпечення зв'язку між пристроями. Проводова інфраструктура використовує мережні кабелі для передачі даних, тоді як безпроводова інфраструктура використовує радіохвилі для бездротового з'єднання.

2.3. Різновиди корпоративних мереж

2.3.1. Локальні мережі (LAN)

Локальна мережа - це мережа, що обмежена географічною областю, такою як офіс, підприємство або кампус. Вона забезпечує спільний доступ до ресурсів та обмін даними між комп'ютерами та пристроями в межах цієї області. Локальні мережі можуть бути проводовими або безпроводовими.

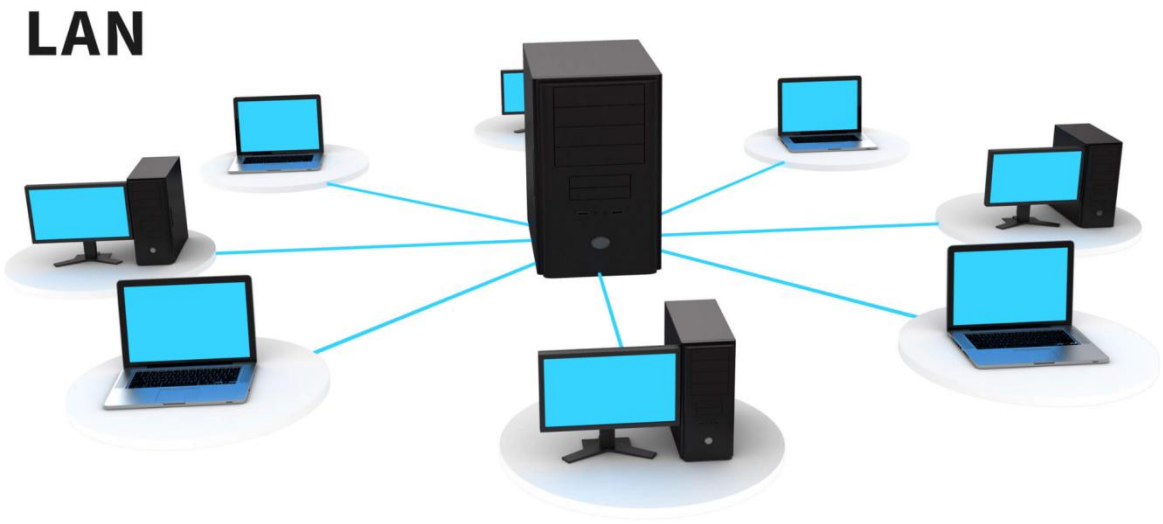

Рисунок 2.3.1 – Схематичне зображення LAN

2.3.2. Глобальні мережі (WAN)

Глобальна мережа - це мережа, що охоплює велику географічну область, таку як кілька офісів або філій розташованих у різних місцях. Глобальні мережі використовують технології передачі даних, такі як приватні мережі, VPN (віртуальні приватні мережі) або Інтернет, для забезпечення зв'язку та обміну

даними між різними локаціями.

Рисунок 2.3.2 – Схематичне зображення WAN

2.3.3. Хмарні мережі

Хмарні мережі використовують хмарні сервіси та інфраструктуру для забезпечення мережевих послуг. Вони дозволяють організаціям використовувати віртуальні ресурси, які розташовані на віддалених серверах, для забезпечення

доступу до даних та послуг з будь-якого місця і пристрою з підключенням до Інтернету.

2.3.4. Віртуальні приватні мережі (VPN)

Віртуальна приватна мережа - це захищений канал комунікації, який дозволяє співробітникам підключатися до корпоративної мережі з віддалених місць через публічну мережу, таку як Інтернет. VPN забезпечує шифрування даних та конфіденційність інформації під час їх передачі, що робить їх безпечними для використання у віддалених офісах або під час подорожей.

2.4. Вразливості компонентів корпоративних мереж

Компоненти мережі, такі як мережеві пристрої, сервери та клієнтські пристрої, є необхідними елементами інфраструктури, що забезпечують передачу даних, зберігання і обробку інформації в організаційному середовищі. Однак, разом зі зростанням складності мережевих технологій та залежності організацій від інформаційних систем, з’являються нові загрози безпеці, пов'язані з вразливостями компонентів мережі. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережевих ресурсів, крадіжки конфіденційних даних, завдання шкоди інфраструктурі або перешкоджання нормальному функціонуванню систем.

Враховуючи серйозні наслідки, які можуть виникнути внаслідок експлуатації вразливостей компонентів мережі, важливо ретельно вивчати цю проблематику і приділяти належну увагу питанням безпеки. Розуміння типових вразливостей, їх причин та наслідків є важливим етапом в розробці ефективних заходів захисту, що дозволить забезпечити надійну безпеку мережевої інфраструктури.

2.4.1. Вразливості маршрутизаторів

Маршрутизатори є основою корпоративних мереж і відповідають за передачу даних між різними сегментами мережі. Однак, вони можуть мати різноманітні вразливості, які можуть бути використані зловмисниками для злому системи та отримання несанкціонованого доступу. Одна з найпоширеніших вразливостей маршрутизаторів полягає у використанні застарілого або недостатньо оновленого програмного забезпечення. Зловмисники можуть використовувати відомі вразливості у програмному забезпеченні маршрутизатора, щоб зламати його і отримати доступ до мережевих ресурсів. Також, некоректна конфігурація маршрутизатора може дозволити несанкціонований доступ до мережі або витік конфіденційної інформації.

Атаки на маршрутизатори можуть бути різноманітні. Наприклад, атаки на переповнення буфера можуть бути використані для перекриття мережевого трафіку та навіть призвести до відмови в обслуговуванні. Зловмисники можуть відправляти шкідливі пакети з метою переповнення буфера маршрутизатора, що призводить до його перевантаження та втрати продуктивності.

Додатково, протоколи маршрутизації також можуть мати свої вразливості. Атаки на маршрутизатори можуть використовувати недоліки у роботі протоколів, таких як OSPF (Open Shortest Path First) або BGP (Border Gateway Protocol), для злому мережі. Зловмисники можуть надсилати фальшиві маршрути або модифікувати маршрути, що призводить до перенаправлення трафіку до небезпечних мереж або відмови в обслуговуванні.

2.4.2 Вразливості комутаторів

Комутатори є іншим важливим компонентом корпоративних мереж, вони забезпечують комутацію пакетів даних і передачу даних в межах локальної

мережі. Проте, комутатори також можуть бути вразливими до різних видів атак, які можуть порушити безпеку мережі.

Одна з найпоширеніших вразливостей комутаторів пов'язана з некоректною конфігурацією. Недостатньо захищена конфігурація може призводити до витоку даних, несанкціонованого доступу до мережевих ресурсів або можливості впровадження фальшивих пристроїв у мережу.

Одним з типів атак на комутатори є атаки на отримання контролю над комутатором. Зловмисники можуть намагатися отримати несанкціонований доступ до комутатора для перехоплення або модифікації мережевого трафіку. Це може призвести до перенаправлення трафіку до зловмисницьких серверів, збору конфіденційної інформації або навіть викликати відмову в обслуговуванні. Крім того, атаки на комутатори можуть включати використання фізичних портів комутатора для підключення фальшивих пристроїв. Це дає зловмисникам можливість відправляти або перехоплювати мережевий трафік без знання адміністраторів мережі.

2.4.3 Вразливості серверів

Сервери в корпоративних мережах зазвичай містять важливу і конфіденційну інформацію, тому вони є привабливими цілями для зловмисників. Вразливості серверів можуть бути різноманітні і пов'язані з як апаратними, так і програмними аспектами.

Однією з найпоширеніших вразливостей серверів є недостатньо оновлене або неправильно налаштоване програмне забезпечення. Застарілі версії операційних систем, веб-серверів, баз даних та інших компонентів сервера можуть містити вразливості, які зловмисники можуть використовувати для злому системи. Крім того, неправильна конфігурація серверів може призводити до витоку конфіденційної інформації, відмови в обслуговуванні або навіть повного контролю зловмисників над сервером.

Сервери також можуть бути вразливі до різних типів атак, таких як атаки на переповнення буфера, SQL-ін'єкції, кросс-сайтові скриптинг та багато інших. Атаки на переповнення буфера використовуються для перекриття роботи сервера шляхом передачі шкідливих даних, які перевищують розмір буфера, що може призвести до відмови в обслуговуванні або виконання віддалених кодів зловмисником. SQL-ін'єкції дозволяють зловмиснику виконувати шкідливі SQL-запити до бази даних сервера, що може призвести до розкриття, модифікації або видалення конфіденційних даних.

2.4.4 Вразливості клієнтів

Вразливості клієнтської сторони корпоративних мереж можуть представляти значну загрозу для безпеки організацій. Користувачі, які використовують клієнтські пристрої, такі як комп'ютери, ноутбуки, смартфони або планшети, можуть бути піддаються різноманітним атакам та інцидентам безпеки, що можуть спричинити витік конфіденційної інформації, пошкодження даних або навіть злам системи.

Одна з основних вразливостей полягає у слабких паролях і незахищених облікових записах. Багато користувачів використовують прості паролі або використовують один і той же пароль для декількох облікових записів, що створює ризик підбору пароля або витоку облікових даних.

Додаткова вразливість полягає в шкідливому програмному забезпеченні, такому як віруси, троянські програми та шпигунське ПЗ. Користувачі можуть несвідомо завантажувати шкідливе ПЗ з інтернету, відкривати вірусні вкладення в електронних листах або використовувати небезпечні програми, що можуть використовувати вразливості у системі.

Помилки користувачів також можуть бути джерелом вразливостей. Наприклад, небезпечне поведінка, таке як відкриття невідомих посилань або

неперевірена передача конфіденційної інформації через незахищені канали комунікації, може стати початком атаки.

Вразливості в операційних системах та програмах можуть бути використані для зламу системи або здійснення несанкціонованого доступу.

2.4.5 Проводова та безпровідна інфраструктура

Вразливості проводової та безпровідної інфраструктури, що використовуються в корпоративних мережах, є серйозними проблемами безпеки, які можуть призвести до несанкціонованого доступу, витоку конфіденційної інформації та порушення нормальної роботи мережі.

Проводова інфраструктура може бути вразливою через недостатні заходи фізичної безпеки. Наприклад, неконтрольований доступ до мережевих пристроїв або підключення до мережевих кабелів може дозволити зловмисникам перехоплювати чи модифікувати передачу даних. Крім того, слабка аутентифікація адміністратора мережі або недостатні заходи захисту паролів можуть дозволити зловмисникам отримати несанкціонований доступ до мережевих ресурсів.

У безпровідній інфраструктурі також існують ризики безпеки. Один з них полягає в використанні слабкого або застарілого протоколу шифрування, що може дозволити зловмисникам перехоплювати та розшифровувати передані дані. Крім того, недостатні заходи захисту паролів для точок доступу можуть стати точкою входу для несанкціонованого доступу до мережі. Зловмисник може використовувати підроблені точки доступу або виконувати атаки типу "Man-in-the-Middle", перехоплюючи комунікацію між пристроями.

Вразливості проводової та безпровідної інфраструктури також можуть бути пов'язані з певними мережевими протоколами або службами. Наприклад, використання застарілих версій протоколів може мати вразливості, які можуть бути використані для атак. Крім того, недостатнє оновлення програмного

забезпечення на мережевих пристроях може призвести до виникнення вразливостей, які можуть бути використані зловмисниками для атак на мережу.

2.5 Вразливості типів корпоративних мереж

2.5.1 Локальна мережа (LAN)

Локальна мережа є внутрішньою мережею організації та зазвичай має обмежений масштаб. Вразливості LAN-мереж включають:

- Недостатня аутентифікація: Використання слабких методів аутентифікації може дозволити несанкціонованим особам отримати доступ до мережі та ресурсів.
- Несанкціонований доступ: Недостатні заходи забезпечення фізичної безпеки можуть дозволити несанкціонованим особам фізично підключитися до мережевих пристроїв або кабелів, що призводить до компрометації мережі.
- Перехоплення пакетів: Відсутність або недостатнє шифрування може дозволити зловмисникам перехоплювати та переглядати мережевий трафік, що може призвести до розкриття конфіденційної інформації.

2.5.2 Глобальна мережа (WAN)

Глобальна мережа охоплює великі географічні області та зазвичай базується на інтернет-протоколах. Вразливості WAN-мереж включають:

- Віддалений доступ: Недостатньо захищені механізми віддаленого доступу можуть стати вразливістю для атак, таких як перехоплення паролів, атаки "брутфорс" (brute-force) або використання вразливостей протоколів.

- Атаки на мережевий периметр: Зловмисники можуть спробувати атакувати мережевий периметр, використовуючи методи, такі як атаки на фаервол, DDoS або використання вразливостей в мережевих пристроях.
- Віртуальні приватні мережі (VPN): Використання недостатньо захищених VPN може викласти мережу ризику. Вразливості VPN можуть включати слабке шифрування, недостатню автентифікацію або використання застарілих протоколів.

РОЗДІЛ 3. КОМПЛЕКСНА БЕЗПЕКА В СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

Комплексна безпека є концепцією, що охоплює широкий спектр заходів, які спрямовані на захист корпоративних мереж від загроз та забезпечення надійності, цілісності та конфіденційності інформації. Вона передбачає впровадження комплексу технічних, організаційних та процесних заходів, що допомагають уникнути загроз безпеці та ефективно реагувати на них.

У даному розділі розглядається поняття комплексної безпеки в контексті корпоративних мереж. Описується його суть, цілі та основні принципи. Далі розглядаються підходи до комплексної безпеки, стандартизація та рамки регулювання в цій області.

3.1 Поняття комплексної безпеки

Комплексна безпека є концепцією, що охоплює широкий спектр заходів, спрямованих на захист корпоративних мереж від загроз та забезпечення надійності, цілісності та конфіденційності інформації. Вона передбачає впровадження комплексу технічних, організаційних та процесних заходів, що допомагають уникнути загроз безпеці та ефективно реагувати на них.

Комплексна безпека в корпоративних мережах має на меті забезпечити захист інформації та ресурсів від несанкціонованого доступу, недобросовісних дій та загроз зовнішнього та внутрішнього походження. Вона включає в себе широкий спектр заходів, таких як захист мережевого периметру, ідентифікація та аутентифікація користувачів, криптографічне захищення інформації, контроль доступу, моніторинг та виявлення вторгнень, резервне копіювання та відновлення даних, аудит безпеки та інші.

3.1.1 Цілі комплексної безпеки

Головною метою комплексної безпеки є забезпечення безпеки корпоративних мереж, включаючи захист інформації, ресурсів та інфраструктури, забезпечення неперервності бізнес-процесів та мінімізація можливих збитків. Деякі з основних цілей комплексної безпеки включають:

- Захист конфіденційності: Забезпечення конфіденційності інформації шляхом використання шифрування, контролю доступу та інших заходів.
- Забезпечення цілісності: Гарантування цілісності даних та ресурсів шляхом виявлення та запобігання несанкціонованим змінам чи втручанням.
- Забезпечення доступності: Забезпечення доступності інформації та ресурсів для легітимних користувачів та виконання бізнес-процесів без перебоїв.
- Забезпечення неперервності бізнесу: Запобігання та відновлення від наслідків аварій, вторгнень та інших негативних подій, що можуть призвести до припинення роботи організації.

3.1.2 Принципи комплексної безпеки

Комплексна безпека базується на декількох ключових принципах, що допомагають досягти ефективного захисту корпоративних мереж:

- Принцип захисту в глибину: Включає в себе використання шарування заходів безпеки на різних рівнях, щоб ускладнити проникнення та поширення загроз.
- Принцип найменшого привілею: Забезпечує обмеження привілеїв користувачів та процесів до мінімуму, що допомагає запобігти несанкціонованому доступу та зловживанням.

- Принцип контролю доступу: Включає в себе встановлення механізмів для ідентифікації, аутентифікації та авторизації користувачів, а також обмеження їх доступу до ресурсів відповідно до їхніх прав та ролей.
- Принцип неперебивності: Передбачає використання резервування, резервного копіювання та механізмів відновлення для забезпечення неперервності бізнес-процесів в разі аварійних ситуацій.

3.2 Підходи до комплексної безпеки

У сфері комплексної безпеки існує кілька основних підходів, які використовуються для забезпечення безпеки корпоративних мереж. Деякі з них включають:

- Система ідентифікації та аутентифікації: Використання механізмів для ідентифікації користувачів (наприклад, логіни, паролі) та їх аутентифікації (наприклад, двофакторна аутентифікація), щоб забезпечити впізнавання та перевірку легітимності користувачів перед наданням доступу до ресурсів.
- Криптографічний захист: Використання шифрування для захисту конфіденційності та цілісності інформації, що передається по мережі.
- Фаєрволи та системи виявлення вторгнень: Встановлення файрволів, які контролюють трафік, що входить і виходить з мережі, та систем виявлення вторгнень, які аналізують мережевий трафік на предмет виявлення аномальних або підозрілих активностей.
- Управління правами доступу: Встановлення політик та механізмів для управління правами доступу користувачів до ресурсів, обмеження привілеїв та контролю виконання приватного коду.
- Моніторинг та аудит безпеки: Використання систем моніторингу для виявлення потенційних загроз та аномальних активностей в мережі, а

також аудиту безпеки для оцінки ефективності заходів безпеки та виявлення слабких місць.

3.3 Стандартизація та рамки регулювання

Стандартизація в галузі комплексної безпеки в корпоративних мережах відіграє важливу роль у забезпеченні єдиної методології та підходів до безпеки. Деякі з основних стандартів та рамок, що використовуються в цій області, включають:

1. ISO/IEC 27001: Стандарт, що визначає вимоги до систем управління інформаційною безпекою та надає рекомендації щодо впровадження відповідних заходів безпеки.
2. NIST Cybersecurity Framework: Рамка, розроблена Національним інститутом стандартів та технологій США, яка надає рекомендації щодо визначення, впровадження та покращення системи кібербезпеки в організаціях.
3. PCI DSS: Стандарт безпеки даних галузі платіжних карток, що встановлює вимоги до організацій, які обробляють платіжні дані, з метою запобігання крадіжці та зловживанням.
4. CIS Critical Security Controls: Список рекомендованих заходів безпеки, розроблений Центром кібербезпеки CIS (Center for Internet Security), які допомагають організаціям запобігти широкому спектру кіберзагроз.

Ці стандарти та рамки регулювання допомагають організаціям впроваджувати найкращі практики в галузі комплексної безпеки та забезпечувати відповідність до встановлених норм та вимог.

3.4 Ключові аспекти та стратегії захисту

Поділ на стратегії захисту в сучасних корпоративних мережах є надзвичайно важливим аспектом, оскільки зростаючі загрози від кібератак та інших форм злочинної діяльності вимагають постійного забезпечення захисту мережевих ресурсів і даних. Ключові аспекти та стратегії комплексної безпеки у сучасних корпоративних мережах:

- Фізична безпека: Забезпечення фізичної безпеки мережевої інфраструктури є першим кроком у комплексній безпеці. Це включає фізичний доступ до мережевих пристроїв, серверних кімнат, дата-центрів та інших просторів. Контроль доступу, системи відеоспостереження, бар'єри та інші заходи забезпечення фізичної безпеки допомагають запобігти несанкціонованому доступу та зберегти обладнання і дані.
- Мережева безпека: Забезпечення безпеки на рівні мережі включає в себе використання захисних механізмів, таких як фаерволи, системи виявлення і запобігання вторгнень (IDS/IPS), віртуальні приватні мережі (VPN) і маршрутизація на основі політик. Встановлення та налаштування цих захисних систем допомагає уникнути несанкціонованого доступу, перехоплення даних і розповсюдження шкідливих програм.
- Безпека даних: Захист даних є критично важливим аспектом комплексної безпеки. Включається шифрування даних, контроль доступу на основі ролей, резервне копіювання і відновлення даних, а також моніторинг активності користувачів. Додаткові заходи, такі як механізми контролю цілісності даних і аудит безпеки, допомагають виявляти й реагувати на можливі порушення безпеки.
- Безпека користувачів: Люди є слабким ланцюгом у комплексній безпеці, тому надання належної уваги безпеці користувачів є критично важливим. Налагодження строгих політик паролів, навчання користувачів щодо безпечних практик використання інтернету, проведення свідомих

регулярних навчань з питань кібербезпеки та механізми аутентифікації (наприклад, двофакторна аутентифікація) допомагають уникнути атак, пов'язаних з соціальним інженерингом і скомпрометуванням облікових записів користувачів.

- Моніторинг і виявлення: Регулярний моніторинг мережі та систем дозволяє виявляти аномальну активність, потенційні загрози та вразливості. Використання моніторингових інструментів, системи журналювання подій та аналізу безпеки допомагає вчасно виявляти і реагувати на інциденти безпеки.
- Оновлення і патчі: Регулярне оновлення програмного забезпечення, операційних систем та застосунків є важливим аспектом комплексної безпеки. Патчі виправляють відомі вразливості, заповнюють "дірки" безпеки та зменшують ризик успішної атаки.

3.5 Реалізація безпеки в корпоративній мережі згідно з принципами OSI моделі

3.5.1 Фізичний рівень

Фізичний рівень, відомий також як physical layer, забезпечує передачу бітів через різні фізичні канали зв'язку, такі як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. Цей рівень відповідає за характеристики фізичного середовища передачі даних, такі як пропускна здатність, захист від перешкод, хвильовий опір і інші параметри. Крім того, фізичний рівень встановлює характеристики електричних сигналів, які передають дискретну інформацію, такі як швидкість передачі сигналів, тип кодування, крутизна фронтів імпульсів, рівні напруги або струму.

Усі пристрої, що підключені до мережі, реалізують функції фізичного рівня. З боку комп'ютера ці функції виконуються мережевим адаптером або послідовним портом.

Один з прикладів протоколу фізичного рівня - специфікація 10BaseT технології Ethernet. Ця специфікація встановлює стандарти для типу кабелю, який використовується (наприклад, неекранована вита пара з хвильовим опором 100 Ом), роз'єму RJ-45, максимальної довжини фізичного сегмента (100 метрів), використання манчестерського коду для представлення даних в кабелі та інших характеристик середовища і електричних сигналів.

Деякі з найпоширеніших специфікацій фізичного рівня включають:

- EIA-RS-232-C, CCITT V.24/V.28 - механічні та електричні характеристики незбалансованого послідовного інтерфейсу;
- EIA-RS-422/449, CCITT V.10 - механічні, електричні та оптичні характеристики збалансованого послідовного інтерфейсу;
- IEEE 802.3 - Ethernet;
- IEEE 802.5 - Token ring.

Ці специфікації встановлюють стандарти і параметри для фізичних рівнів відповідних мережевих протоколів, що дозволяють ефективно передавати дані через фізичні медіа зв'язку.

Фізичний рівень мережі виконує роль транспортування бітів кадра через мережеве середовище. Цей рівень отримує кадри від канального рівня та перетворює їх в імпульси, що передаються через фізичні середовища, такі як електричні, світлові або мікрохвильові сигнали. Середовище передає не кадри в цілому, а поодинокі сигнали, що представляють окремі біти кадра.

Фізичний рівень також може включати додаткові сигнали для вказівки початку та кінця кадра. Стандарти для фізичного рівня розробляються організаціями, такими як ITU, IEEE, ISO, ANSI, EIA/TIA, FCC, і реалізуються в мережевих адаптерах пристроїв. Ці стандарти охоплюють чотири області фізичного рівня: фізичні й електричні властивості середовища, механічні

властивості конекторів, представлення бітів у вигляді сигналів та визначення службових сигналів.

Основні функції фізичного рівня включають фізичні компоненти, кодування даних (encoding) для приведення бітів кадра до визначеного вигляду, сигналізацію (signaling) в середовище за допомогою сигналів та визначення часу біта (bit time) – часу, який займає один біт в середовищі передачі. Біти можуть бути представлені за допомогою зміни амплітуди, частоти або фази сигналу.

Наприклад, одним з методів кодування є NRZ (Non-Return-to-Zero), де використовуються різні рівні напруги для представлення 0 та 1. Існує також манчестерське кодування, де 0 та 1 представлені зміною напруги в середині часу біта. Для забезпечення надійності передачі бітів їх можна попередньо кодувати за допомогою кодових груп, що дозволяє виявляти та виправляти помилки.

Щодо передачі даних, вона може бути оцінена за такими характеристиками: смуга пропускання (bandwidth) – кількість інформації, яку можна передати через середовище протягом певного часу, пропускна здатність (throughput) – кількість бітів, що передаються протягом певного часу, та корисне навантаження (goodput) – кількість корисних даних користувача, переданих протягом певного часу.

Існують різні види передавальних середовищ, які використовуються для створення комп'ютерних мереж. Один з таких видів - мідний кабель, але він має недолік у чутливості до електромагнітних перешкод. Для захисту від цих перешкод застосовуються екрановані типи мідних кабелів.

Неекранована вита пара (UTP) складається з 4 або 2 пар проводів, які перекручуються між собою, щоб зменшити вплив перешкод (міжпровідникового перехресного завади). Кожна пара має свій власний колір, що допомагає однозначно ідентифікувати пару на обох кінцях кабелю. Для підключення використовується конектор RJ-45. Існують два стандарти для розташування контактів у конекторі - T568A і T568B.

Прямий кабель (straight-through) - обидва кінці кабелю мають однакову конфігурацію контактів. Використовується для з'єднання різних пристроїв, наприклад, комп'ютера з комутатором або маршрутизатором з комутатором.
Схрещений кабель (crossover) - кінці кабелю мають різну конфігурацію контактів. Використовується для з'єднання однакових пристроїв, наприклад, комутатора з комутатором, маршрутизатора з маршрутизатором або комп'ютера з комп'ютером.

Кабель для консольного з'єднання (rollover) - використовується для підключення до консольних портів мережевого обладнання Cisco. Його один кінець має роз'єм RJ-45, а інший - роз'єм COM/USB.

Коаксіальний кабель складається з центральної жилки і зовнішнього екрану. Раніше він використовувався для локальних мереж, але зараз застосовується переважно у кабельному телебаченні.

Екранована вита пара (STP) - кожна пара проводів має окремий екран, а також загальний екран. Раніше цей тип кабелю використовувався для мереж Token Ring, але зараз застосовується для мереж 10G Ethernet.

Мідний кабель може бути небезпечним, якщо він підключений до несправного обладнання або під час грози, оскільки може виникнути електричний розряд. Крім того, при горінні оболонки кабелю можуть виділятися токсичні речовини.

Оптичний кабель (волоконно-оптичний кабель) складається з центральної скляної жилки, по якій передається світло. Він використовується для передачі даних на великі відстані, не піддається електромагнітній інтерференції і забезпечує високу швидкість передачі. Для передачі даних можуть використовуватися як одномодові кабелі з тонкою центральною жилою (8-10 мікронів), які дозволяють передавати сигнали на відстань до 100 км, так і багатомодові кабелі з товстою центральною жилою (50 мікронів), які підходять для відстаней до 2 км.

Забезпечення безпеки на фізичному рівні передбачає збереження структурної цілісності мережі, що означає її неподільність. Головними загрозами для структурної цілісності мережі є:

- Несанкціонований доступ до ресурсів мережі через проникнення в систему.
- Фізичне пошкодження мережі.
- Створення завад у безпровідних каналах передачі даних.

Здійснення цих загроз передбачає наявність попередніх знань про структуру мережі. Порушник, який намагається проникнути в систему, має відповідати таким вимогам:

- Мати обладнання, яке сумісне з обладнанням мережі.
- Бути здатним розпізнавати структуру і параметри сигналу.
- Мати знання про параметри мережі, такі як ідентифікатор мережі, інфраструктура мережі, адреси, що дозволені в точці доступу.
- Мати шифрувальний ключ (якщо використовується шифрування інформації в мережі)

Окремим видом загрози фізичного впливу є створення завад у мережі. Ця атака може бути здійснена, якщо зловмисник має інформацію про засоби безпроводового зв'язку, параметри сигналу, режим роботи. Для досягнення цього, зазвичай проводиться радіотехнічний моніторинг, після чого на основі отриманих даних створюються завади. Вузлові об'єкти, такі як ретранслятори, репітери, базові станції, центри комутації, є особливо вразливими елементами системи. Вплив на них може спричинити відмову безпроводового зв'язку в певній зоні обслуговування, що збільшує загрозу для системи в цілому.

Служба радіоконтролю частотних ресурсів застосовує адміністративні методи для боротьби з джерелами завад. Її завдання включає розробку заходів, спрямованих на припинення випромінювання джерел завад, які перешкоджають нормальному функціонуванню зареєстрованих радіозасобів.

Згідно рекомендацій Міжнародного союзу електрозв'язку (МСЕ), ці заходи можуть включати:

- Переміщення окремих каналів у багатоканальній системі передачі.
- Використання направлених антен.
- Припинення роботи однієї зі станцій, яка є джерелом завад для інших.
- Коригування розкладів або експлуатаційних угод (розділення за часом).
- Зміну класу випромінювання.
- Зміну частоти.
- Перенесення навантаження на інші наявні частоти.

Проте організаційні методи не можуть повністю усунути можливість дії завад. Тому для досягнення кращої завадостійкості радіозасобів необхідно вживати технічні заходи. Серед таких заходів використовуються методи, що базуються на вибірковому прийманні сигналів за їх просторовим положенням, частотою або поляризацією, а також використання сигналів зі спеціальною структурою, що забезпечує підвищену завадостійкість.

3.5.2 Канальний рівень

На цьому рівні передачі даних забезпечується керування доступом до середовища та пакування протокольних даних в кадри. Кадр є блоком даних, що передається на канальному рівні. Вузол визначає пристрій, який підключений до загального середовища передачі даних. Середовище є фізичним середовищем передачі даних, таким як кабель або радіохвилі. Мережа складається з вузлів, які з'єднані середовищем передачі даних.

Канальний рівень дозволяє протоколам мережного рівня працювати незалежно від конкретних технологій, що використовуються в мережі. Це дає змогу протоколам мережного рівня працювати в різних типах мереж. Протоколи

канального рівня визначають, як пакети інкапсулюються в кадри та як біти розміщуються у середовищі передачі даних.

Протоколи канального рівня також описують методи контролю доступу до середовища, які дозволяють пристроям взаємодіяти з середовищем і передавати кадри в різних мережних середовищах. Фреймування та контроль доступу до середовища керуються мережевими адаптерами пристроїв.

Одним з важливих завдань на канальному рівні є перевірка доступності середовища передачі даних та виявлення й корекція помилок. Це досягається шляхом групування бітів у кадри, які забезпечують правильну передачу кожного з них.

Структура кадру може різнитися в залежності від протоколу, що використовується на канальному рівні. У заголовку кадру містяться основні поля, такі як початок кадру, адреси та довжина кадру або тип протоколу на третьому рівні.

У випадку точка-точка з'єднань передача кадрів може обійтися без адресації, оскільки такі кадри можуть мати лише одну адресу призначення, яка є широкомовною. Але при використанні множинного доступу до середовища необхідно вказувати як адресу джерела, так і адресу призначення для успішної доставки. У кінцевику кадрі може міститися контрольна сума, наприклад, CRC, яка дозволяє перевірити цілісність кадру вузлом приймання. Крім того, кінцевик містить біти, що позначають кінець кадру.

З погляду інформаційної безпеки, канальний рівень досить добре вивчений і відповідає за формування та доставку кадрів без помилок. На цьому рівні використовується апаратна адресація MAC та здійснюється обчислення контрольної суми. Зловмисники широко використовують атаки на підміну MAC-адреси, атаки на протоколи ARP і Spanning-Tree, з метою перехоплення трафіку та отримання доступу до конфіденційної інформації. Також існує загроза захоплення всіх портів VLAN, використовуючи можливості побудови віртуальних мереж VLAN на комутаторах. Розповсюдження безпроводових

мереж стандарту IEEE 802.11 створило ризик безконтрольного підключення зловмисників до цих мереж.

Один з ключових ризиків, пов'язаних з вразливістю протоколів канального рівня у моделі OSI, полягає в тому, що зламування мережі на цьому рівні може відкрити можливість для зловмисника обійти та оминути вжиті заходи захисту, які встановлені та застосовуються на вищих рівнях. Це може мати серйозні наслідки, зокрема створюючи потенційну вразливість для несанкціонованого доступу до мережних ресурсів та конфіденційної інформації.

Розглянемо різні типи атак на канальному рівні локальних обчислювальних мереж:

Пасивні атаки:

- Прослуховування (sniffing) та аналіз мережевого трафіку використовують недоліки в протоколах і мережному устаткуванні. За допомогою сніфера можна отримати різноманітну інформацію, включаючи конфіденційну, таку як імена користувачів і паролі.
- Підміна довіреного суб'єкта використовує можливість некоректного привласнення IP- або MAC-адреси або підміни цих адрес відправника іншими адресами. Цей вид атаки називають фальсифікацією адреси.

Активні атаки:

- Відмова в обслуговуванні (Denial of Service, DOS) має на меті паралізувати мережу або її ресурси, щоб заборонити звичайному користувачеві отримати доступ до них. Атака DOS перевищує допустимі межі функціонування ресурсів мережі, операційної системи або застосунків, при цьому використовуються протоколи TCP і ICMP. Деякі з відомих видів атаки DOS включають TCP SYN Flood та Ping of Death.
- Порушення роботи мережі або її ділянок відбувається через недоліки протоколів канального рівня, які можуть призвести до розхитання відмовостійкості мережі або її частини. Наприклад, переповнення таблиці комутації може спричинити некоректну роботу протоколів.

Для протидії зазначеним загрозам на канальному рівні можна використовувати наступні заходи:

-Застосування MAC-фільтрації для контролю доступу до мережевих ресурсів.

-Використання брандмауерів для ізоляції різних зон у мережі та відмова від використання VLAN.

-Застосування шифрування, автентифікації та фільтрації MAC-адрес для безпроводових мереж.

-Ці заходи допоможуть зменшити ризик вразливості та забезпечити більшу безпеку на канальному рівні локальних обчислювальних мереж.

3.5.3 Мережний рівень

Мережевий рівень вважається найбільш вразливим з точки зору захисту. На цьому рівні формується вся маршрутизована інформація, відправники і одержувачі вказуються явно, а також здійснюється управління потоком. Протоколи мережевого рівня опрацьовують пакети на всіх маршрутизаторах, шлюзах та інших проміжних вузлах. Більшість специфічних мережевих атак використовують протоколи цього рівня, такі як читання, модифікація, знищення, дублювання, переорієнтація повідомлень або потоку, а також маскування під інший вузол. Захист від таких загроз здійснюється за допомогою протоколів мережевого і транспортного рівнів та криптографічних засобів. Крім того, на мережевому рівні може бути використана вибіркова маршрутизація.

Протоколи канального рівня локальних мереж забезпечують доставку даних між вузлами в мережах з певною топологією. Це обмеження не дозволяє створювати мережі з складною структурою. Тому для забезпечення простоти процедур передачі даних у типових топологіях і дозволу використання довільних топологій було введено додатковий мережевий рівень. На мережному рівні сам термін "мережа" отримує специфічне значення, що означає сукупність

комп'ютерів, з'єднаних у відповідності з однією з типових топологій та використовуються для передачі даних одним з протоколів канального рівня, визначених для цієї топології. В межах мережі доставка даних забезпечується канальним рівнем, а передачу даних між мережами здійснює мережевий рівень, який дозволяє вибрати найкращий маршрут передачі. Для передачі повідомлення від відправника, розташованого в одній мережі, до отримувача в іншій мережі необхідно здійснити кілька транзитних передач між мережами, вибираючи найкращий маршрут кожного разу. Мережевий рівень використовує такі засоби для передачі даних між вузлами по мережі:

- Адресацію.
- Інкапсуляцію/декапсуляцію.
- Маршрутизацію.

Деякі протоколи мережного рівня включають IPv4, IPv6, IPX, Appletalk, CLNS/Decnet. Характеристики протоколу IPv4 включають його безз'єднаність, ненадійність (не гарантує доставку), незалежність від середовища передачі (за винятком MTU, де канальний рівень повідомляє мережевому рівню про максимальний розмір блоку передачі). При перевищенні розміру MTU пакет може бути фрагментований перед передачею.

Замість того, щоб тримати всі пристрої в одній мережі, більш практично розподіляти їх у групи, що дозволяє:

- Групувати вузли залежно від їхнього місцезнаходження, наприклад, на одному поверсі або в одному будинку.
- Групувати вузли залежно від їхніх цілей та типів трафіку, який вони обробляють.
- Групувати вузли залежно від їхньої приналежності до конкретної компанії або відділу.

Розподіл вузлів на групи дозволяє вирішити деякі проблеми, які можуть виникнути в великих мережах, такі як:

- Зниження продуктивності через велику кількість вузлів у одному сегменті, що створює багато широкомовного трафіку та навантажує мережу.
- Погрози безпеки, оскільки в точці переходу з однієї мережі в іншу можна налаштувати обмеження за типом трафіку та адресою.
- Управління адресацією, де вузлам не потрібно зберігати багато маршрутів, а достатньо знати адресу свого шлюзу.

IP-Адреса, яка є 32-бітною та ієрархічною, складається з двох частин:

- Мережева частина, яка вказує на мережу, в якій знаходиться вузол.
- Вузлова частина, яка вказує на конкретний вузол у мережі.

Розмір мережної частини визначається маскою мережі або довжиною префікса.

На мережному рівні можна виділити два основних типи протоколів. Перший тип - це мережні протоколи (routed protocols), які відповідають за пересилання пакетів у мережі. Ці протоколи часто асоціюються з протоколами мережного рівня. Другий тип протоколів, що також належать до мережного рівня, називають протоколами обміну маршрутною інформацією або протоколами маршрутизації (routing protocols). Протоколи мережного рівня реалізуються за допомогою програмних модулів операційної системи, а також програмних та апаратних засобів маршрутизаторів. На мережному рівні також діють протоколи, які відповідають за відображення адрес вузлів, які використовуються на мережевому рівні, у локальні адреси мережі. Прикладами протоколів мережного рівня є протокол міжмережевої взаємодії IP та протокол міжмережевого обміну пакетами IPX.

Для передачі інформації між вузлами, які знаходяться у різних мережах, потрібні маршрутизатори. Маршрутизатори є прикордонними пристроями, які з'єднують мережі одна з одною. Мережі, до яких підключені порти маршрутизатора, вважаються "підключеними" (directly connected). А мережі, до яких підключені сусідні маршрутизатори, вважаються "віддаленими" (remote).

Коли ПК потребує відправити інформацію вузлу, який не знаходиться в його мережі, він направляє цю інформацію своєму шлюзу. Шлюз, який є маршрутизатором, вибирає шлях передачі інформації, користуючись таблицею маршрутів. Під час маршрутизації:

- Порівнюються адреси мереж та адреса призначення побітно. Вибирається адреса з найбільшим збігом бітів.
- Якщо не знайдено жодного відповідного маршруту, використовується маршрут за замовчуванням (default route).
- Якщо немає підходящого маршруту або маршруту за замовчуванням, пакет відкидається, а на адресу джерела надсилається повідомлення про помилку. Якщо в таблиці маршрутизації є підходящий маршрут, визначається сусід, який відповідає цій мережі, та інтерфейс маршрутизатора, через який він доступний. Пакет пересилається до сусіда.
- Маршрутизатори змінюють заголовок кадра під час передачі його з одного інтерфейсу на інший, оскільки інтерфейси можуть використовувати різні протоколи. MAC-адреси не містять інформацію про мережу.

3.5.4 Транспортний рівень

Транспортний рівень виконує кілька важливих ролей у мережі. Він відповідає за відстеження індивідуальних сеансів та мультиплексування їх, сегментування даних для передачі, складання сегментів у вихідний блок даних та ідентифікацію додатків за номерами портів. З огляду на різні вимоги різних додатків, на транспортному рівні використовуються різні протоколи.

Протоколи транспортного рівня надають різноманітні функції, такі як орієнтовані на з'єднання сеанси, надійність доставки, реконструкцію даних по номерах сегментів та контроль потоку. Для забезпечення надійності доставки протоколи використовують облік переданих даних, підтвердження про приймання сегментів та повторне пересилання загублених сегментів. Ці

додаткові службові повідомлення протоколу створюють додаткове навантаження на мережу.

У транспортному рівні існують два основних протоколи: TCP і UDP. TCP використовується для протоколів, які потребують надійну доставку, тоді як UDP використовується для протоколів, які не вимагають надійності доставки.

Для ідентифікації сеансів різних додатків на транспортному рівні використовуються номери портів. Сокет дозволяє унікально ідентифікувати сеанс зв'язку за допомогою комбінації IP-адреси та номера порту. Номери портів призначає організація IANA, і вони поділяються на три категорії: добре відомі (0–1023), які закріплені за популярними протоколами; зареєстровані (1024–49151), які можуть бути видані розробниками протоколів без обігу в IANA; динамічні або приватні (49152–65535), які використовуються тимчасово при встановленні сеансу зв'язку.

Команда "netstat" надає зручний спосіб перегляду списку відкритих сеансів TCP у операційній системі, а також відображає порти, які служби прослуховують.

Безпека на транспортному рівні OSI (Open Systems Interconnection) є критично важливим аспектом для забезпечення захищеної передачі даних у мережі. Захист транспортного рівня включає в себе заходи безпеки, спрямовані на забезпечення конфіденційності, цілісності та доступності передачі даних.

Один із найпоширеніших протоколів на транспортному рівні, TCP (Transmission Control Protocol), має вбудовані механізми безпеки, такі як контроль цілісності даних за допомогою контрольних сум (checksums) та підтвердження доставки. Однак, для забезпечення додаткових рівнів безпеки можуть використовуватись додаткові протоколи і заходи.

Одним з таких протоколів є SSL/TLS (Secure Sockets Layer/Transport Layer Security), який забезпечує шифрування комунікації між клієнтом і сервером на транспортному рівні. SSL/TLS забезпечує конфіденційність даних шляхом захисту їх від прослуховування та зловживання. Він також використовує

сертифікати для перевірки автентичності сторін та забезпечення надійності комунікації.

Додатковими заходами безпеки на транспортному рівні можуть бути застосування фаєрволів (firewalls) для контролю доступу до мережі і фільтрації пакетів даних, а також використання віртуальних приватних мереж (VPN) для створення безпечного тунелю для передачі даних.

Однак, важливо враховувати, що безпека на транспортному рівні сама по собі не забезпечує повну безпеку мережі. Вона повинна бути поєднана з заходами безпеки на інших рівнях OSI, таких як мережевий та застосунковий рівні, для створення комплексного підходу до безпеки.

Загальною метою безпеки на транспортному рівні є забезпечення надійної та безпечної передачі даних у мережі, запобігання несанкціонованому доступу, а також захист від атак, таких як перехоплення, модифікація або відмова в обслуговуванні. Завдяки належним заходам безпеки на транспортному рівні можна створити надійну та безпечну мережеву інфраструктуру, що задовольняє вимоги сучасного цифрового середовища.

3.5.5 Сеансовий рівень

Сеансовий рівень (рівень сесії) відповідає за встановлення, обслуговування та завершення сесій між додатками. Протокол RPC (Remote Procedure Call) є прикладом протоколу сеансового рівня, який дозволяє виконувати процедури на віддаленому хості. Під час виконання таких процедур встановлюється сеанс з'єднання між додатками, і його призначенням є обслуговування запитів, що виникають під час взаємодії програми-сервера з додатком-клієнтом.

Шлюз сеансового рівня (Session Level Gateway – SLG) є активним транслятором TCP-з'єднання. Він приймає запити авторизованих клієнтів для надання послуг, перевіряє допустимість запиту сеансу (handshaking), встановлює потрібне з'єднання з адресою призначення зовнішньої мережі і збирає статистику

про цей сеанс зв'язку. Після підтвердження того, що клієнт і зовнішній хост є "законними" (авторизованими) учасниками сеансу, шлюз транслює пакети в обох напрямках без фільтрації. Зазвичай пункт призначення визначається заздалегідь, і джерелом інформації може бути багато (з'єднання "один-до-багатьох"), наприклад, використання зовнішнього веб-проксі.

За допомогою різних портів можна створювати різні конфігурації з'єднань для обслуговування всіх користувачів, які мають право на доступ до ресурсів мережі. Проте, важливим недоліком SLG є те, що після встановлення з'єднання пакети фільтруються тільки на сеансовому рівні моделі OSI без перевірки їх вмісту на рівні прикладних програм. Це означає, що авторизований зловмисник може спокійно передавати шкідливі програми через такий шлюз. Тому захист реалізується головним чином за допомогою квитувань (Handshaking).

Протоколи сеансового рівня OSI/ISO забезпечують механізми управління сеансами, включаючи реєстрацію, управління діалогом і обмін параметрами сеансу. Ці протоколи описані в стандартах ISO 8326/CCITT X.215 (визначення і основні характеристики сеансової служби) і ISO 8327/CCITT X.225, які визначають специфікації протоколів:

- BCS - базової комбінованої підмножини;
- BSS - базової підмножини синхронізації;
- BAS - базової підмножини функціонування.

Управління діалогом під час сеансу здійснюється в OSI/ISO за допомогою мітки, надання якої дає право на зв'язок. Мітку можна запитати, і для сеансової служби може бути встановлений пріоритет на використання мітки.

Протоколи рівня представлення OSI/ISO забезпечують прозорий зв'язок ES між прикладними процесами, що працюють на різних комп'ютерних платформах та операційних середовищах. Ці протоколи описані в стандартах ISO 8822/CCITT X.216 (визначення служби) і ISO 8823/CCITT X.226, які визначають специфікацію протоколу, включаючи базові процедури встановлення/закінчення

з'єднання, контекстне управління (вибірка/видалення контексту) та контекстне представлення під час повторної синхронізації або відновлення активності.

Структури даних для абстрактної нотації даних (Abstract Syntax Notation - ASN) визначаються в стандартах ISO 8824/CCITT X.208 (специфікації ASN.1) і ISO 8825/CCITT X.209 (основні правила кодування для ASN.1). Крім того, до рівня представлення належать стандарти представлення кодів символів. Найбільш поширеними стандартами є 7-бітовий код ASCII та його 8-бітове розширення, яке включає символи псевдографіки та букви інших алфавітів, наприклад, кирилицю. Для великих машин IBM використовується двійковий розширений код EBCDIC. Стандарти ISO визначають також 8-бітовий код ISO 8859 і 16-бітовий код 6937 для представлення символів найбільш поширених алфавітів, включаючи ієрогліфи.

Протоколи сеансового рівня і рівня представлення даних відіграють важливу роль у забезпеченні безпеки мережі. На сеансовому рівні безпеку забезпечується за допомогою ідентифікаторів і паролів користувачів. ISO рекомендує застосовувати шифрування на рівні представлення даних для забезпечення безпеки мережі. Для шифрування даних був запропонований стандарт ISO 9797, який визначає механізм цілісності даних за допомогою криптографічної функції перевірки з використанням алгоритму блокового шифрування.

Загалом, протоколи сеансового рівня та рівня представлення даних визначають механізми управління сеансами та забезпечують прозорий зв'язок між додатками, працюючими на різних платформах, а також виконують важливі функції забезпечення безпеки мережі.

Сеансовий рівень в моделі OSI відіграє ключову роль у формуванні захищених віртуальних каналів з найвищим рівнем функціональності для обміну інформацією, контролю доступу та простоти конфігурування системи безпеки. Протоколи на цьому рівні надають безперешкодний доступ до захищених віртуальних мереж для високорівневих протоколів, таких як HTTP, FTP, POP3,

SMTP, NNTP і багатьох інших. Однак, відповідальність за реалізацію захисту інформаційного обміну на сеансовому рівні часто потребує внесення змін до високорівневих мережевих додатків.

На сеансовому рівні моделі OSI встановлюються логічні з'єднання і керуються сполуками, що надає можливість використовувати програми-посередники для перевірки допустимості з'єднань та виконання інших функцій захисту міжмережевої взаємодії. Ці програми-посередники, які часто використовуються в міжмережевих екранах, можуть виконувати різноманітні функції, такі як ідентифікація та автентифікація користувачів, криптозахист переданих даних, розмежування доступу до ресурсів внутрішньої та зовнішньої мереж, фільтрація повідомлень, трансляція адрес та багато інших.

Особливо популярним протоколом криптографічного захисту на сеансовому рівні є SSL/TLS (Secure Sockets Layer/Transport Layer Security), розроблений компанією Netscape Communications. Він надає можливість криптографічного захисту інформаційного обміну, включаючи аутентифікацію, і знаходить широке застосування у безпеці мереж та комунікаційних протоколах.

Безпека на сеансовому рівні моделі OSI є невід'ємною складовою надійної та безпечної мережевої інфраструктури. Цей рівень має надзвичайну вагу, оскільки забезпечує формування та керування захищеними віртуальними каналами для ефективного та безпечного обміну інформацією. Від побудови безпечних віртуальних мереж на сеансовому рівні залежать ключові показники, такі як функціональна повнота захисту інформаційного обміну, надійність контролю доступу та простота конфігурування системи безпеки.

Сеансовий рівень стає основою для впровадження різноманітних протоколів, які забезпечують створення безпечних віртуальних каналів для прикладних протоколів захисту та високорівневих протоколів, що надають різні сервіси, такі як протоколи HTTP, FTP, POP3, SMTP, NNTP та інші. Ці протоколи дозволяють забезпечити прозорість для застосунків і виконувати їхні функції безпеки на сеансовому рівні. Важливо відзначити, що вимагається внесення змін

до високорівневих мережевих додатків для реалізації протоколів захисту інформаційного обміну на цьому рівні, оскільки починається безпосередня залежність від цих додатків.

У процесі формування безпечних віртуальних мереж на сеансовому рівні надається можливість використовувати програми-посередники, що виконують різні функції для забезпечення безпеки та підтримки міжмережевої взаємодії. Ці програми-посередники можуть здійснювати ідентифікацію та автентифікацію користувачів, криптографічний захист переданих даних, розмежування доступу до ресурсів внутрішньої та зовнішньої мереж, фільтрацію та перетворення потоку повідомлень, трансляцію внутрішніх мережевих адрес, реєстрацію подій та реагування на них, а також кешування запитуваних даних з зовнішньої мережі.

У практичному застосуванні найпопулярнішим протоколом для криптографічного захисту інформаційного обміну на сеансовому рівні залишається протокол SSL/TLS. Цей протокол забезпечує конфіденційність, цілісність та автентичність даних, які передаються через мережу, і став стандартом для безпечного з'єднання між клієнтом і сервером.

Враховуючи всі вищезазначені аспекти, безпека на сеансовому рівні моделі OSI має на меті забезпечити надійність, конфіденційність та захист інформації під час її обміну між різними вузлами мережі. Це досягається шляхом застосування відповідних протоколів, програм-посередників та засобів моніторингу, які забезпечують ефективну обробку, контроль та захист даних на сеансовому рівні. При побудові безпечних віртуальних мереж необхідно враховувати специфіку мережевих додатків та вимоги щодо безпеки, забезпечуючи найвищий рівень захисту та забезпечуючи безперебійну та надійну мережеву взаємодію.

РОЗДІЛ 4. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ БЕЗПЕКИ В КОРПОРАТИВНУ МЕРЕЖУ

Упродовж тривалого періоду локальні обчислювальні мережі (ЛОМ) були широко поширеними в організаціях, надаючи можливість спільного використання даних та підключення додаткових пристроїв, таких як принтери. З плином часу, ці мережі почали об'єднуватися між собою, утворюючи новий вид - територіально розподілені мережі (ТРМ), які дозволяють обмін інформацією між географічно віддаленими організаціями.

На сьогоднішній день існує велика кількість ТРМ, серед яких відомі Internet, Relcom та Sovintel, а також спеціалізовані мережі. Початково створений як ARPANET, Інтернет став глобальною інформаційною супермагістраллю, що з'єднує різні комп'ютерні системи. Проект NSFNET, який був підтриманий національним науковим фондом США, вніс великий вклад у розвиток мережі та сприяв міжнародній співпраці.

З поширенням Інтернету комп'ютери, підключені до мережі, можуть використовувати різні операційні системи, такі як Windows (9X, NT), NetWare, OS/2, Mac OS та UNIX. Швидкість обміну даними залежить від багатьох факторів, включаючи конфігурацію комп'ютерів, мережі та навички користувачів. Зазвичай обмін даними здійснюється за допомогою веб-браузерів клієнтів, використовуючи мережеві протоколи, такі як TCP/IP, та HTTP-сервер.
Зростаюча роль Інтернету стала засобом доступу до інформації та швидким глобальним засобом комунікації, що змінило спосіб, яким організації спілкуються та виконують свої завдання. Такі мережі надають можливості для співпраці, обміну ресурсами та спільної роботи над проектами, незалежно від фізичного розташування учасників. Вони стали невід'ємною складовою бізнес-середовища, де організації ефективно використовують свої ресурси та розширюють можливості завдяки глобальному зв'язку.

Формування безпечної мережевої інфраструктури є критично важливим процесом, який потребує ретельного планування і унікального підходу. При налагодженні безпеки в мережі слід звертати особливу увагу на кілька ключових аспектів, зокрема на визначення необхідних сервісів, оцінку ризиків, пов'язаних з ними, та розробку відповідних механізмів для зменшення цих ризиків.

У процесі планування мережевої інфраструктури збільшується обсяг інформації, на основі якої розробляється унікальний дизайн інфраструктури. Важливим етапом є також формулювання політик безпеки, що визначають правила і процедури для забезпечення безпеки мережі.

На наступному етапі впровадження мережі слід приділити належну увагу початковій налаштуванню системи захисту та постійному відстеженню подій безпеки, їх аналізу та оптимізації політик безпеки. Ефективні політики безпеки та їх строге дотримання є критичними для успішної роботи системи захисту. Крім того, документування цих політик та уникнення зайвих винятків є важливим кроком у збереженні безпеки.

Уникнення використання простих паролів, помилок у конфігурації пристроїв, використання налаштувань за замовчуванням, а також незахищених протоколів і технологій вважається необхідними заходами для забезпечення повної безпеки IT-інфраструктури. Рекомендується впровадження механізмів захисту на всіх рівнях мережі, зокрема на кордонних маршрутизаторах та комутаторах доступу. Використання керованих комутаторів з функціями захисту протоколів ARP, DHCP та STP, а також авторизація користувачів за допомогою технології 802.1x та розміщення співробітників у різних VLAN залежно від їх обов'язків є важливими кроками для забезпечення безпеки мережі.

У разі підключення до мережі WAN та Інтернету необхідно використовувати брандмауери, які забезпечують сканування трафіку на рівні додатків та виявлення потенційних загроз за допомогою систем IPS. Захист від атак типу DoS і DDoS також є необхідним для обладнання. У мережі Інтернет можна використовувати проксі-сервери з фільтрацією веб-контенту та

перевіркою наявності шкідливого програмного забезпечення для забезпечення безпеки користувачів. Важливо також мати систему перевірки пошти на наявність спаму і вірусів.

Для безпечного віддаленого доступу рекомендується використовувати технологію VPN з шифруванням передачі даних. Управління мережевим обладнанням повинно здійснюватися за допомогою захищених протоколів SSH, HTTPS та SNMPv3. Синхронізація часу на пристроях є важливою для аналізу журналів. Для отримання інформації про трафік в мережі, завантаженість обладнання та подій можна використовувати протоколи Syslog, RMON, Sflow та NetFlow.

Необхідно також вести облік того, хто, коли і які зміни вносить в конфігурації обладнання. Ретельне планування, впровадження ефективних політик безпеки та використання відповідних заходів захисту на різних рівнях мережі допоможуть забезпечити безпеку інфраструктури і зберегти її унікальний зміст.

Заходи в сфері інформаційної безпеки спрямовані на захист інтересів суб'єктів інформаційних стосунків. Вони фокусуються на трьох основних аспектах: доступності, цілісності та конфіденційності. Ретельне ранжирування та деталізація цих аспектів є початковим кроком при побудові ефективної системи інформаційної безпеки для організацій.

Важливість проблем інформаційної безпеки можна пояснити двома ключовими причинами. По-перше, цінність накопиченої інформації є надзвичайно великою. Пошкодження важливих даних, крадіжка конфіденційної інформації або відмова інформаційних систем можуть призвести до серйозних фінансових збитків і завдати шкоди репутації організації. Більше того, проблеми з інформаційними системами, такими як системи управління або медичні системи, можуть загрожувати життю та здоров'ю людей.

По-друге, існує критична залежність від інформаційних технологій. Сучасні інформаційні системи є складними і потенційно небезпечними, навіть без

урахування дій зловмисників. Постійно з'являються нові вразливості у програмному забезпеченні, а різноманітність апаратних та програмних компонентів додає складності. Принципи побудови корпоративних інформаційних систем змінюються, використовуються зовнішні інформаційні сервіси, аутсорсинг та активні агенти, що додатково підсилює складність проблеми.

Швидкий ріст витрат на захисні заходи та збільшення кількості порушень інформаційної безпеки свідчать про складність цієї проблематики. Для досягнення успіху в цій галузі необхідний комплексний підхід, який охоплює законодавчі, адміністративні, процедурні та технічні заходи. Важливо враховувати не лише технічні аспекти, а й розробляти належну законодавчу базу, залучати керівництво організацій, виділяти необхідні ресурси та забезпечувати заходи управління персоналом та фізичного захисту. Для вирішення цих проблем потрібна ефективна співпраця фахівців з різних галузей знань.

Законодавчий рівень є надзвичайно важливим для забезпечення безпеки інформації. Визнання цієї проблеми і спрямування ресурсів на ключові напрямки досліджень, освітню діяльність і формування негативного ставлення до порушників інформаційної безпеки є вкрай необхідними. На законодавчому рівні встановлюються правові акти і стандарти, які грають ключову роль у цій сфері.

Прикладом значущого законодавства в галузі інформаційної безпеки є американське законодавство, яке є більш розгорнутим і складним порівняно з російським. Серед визначених стандартів також варто відзначити "Помаранчеву книгу", рекомендації X.800 і "Критерії оцінки безпеки інформаційних технологій".

"Помаранчева книга" містить основні поняття та класифікацію інформаційних систем з точки зору безпеки. Рекомендації X.800 детально розглядають питання захисту мережевих конфігурацій і пропонують широкий

спектр сервісів і механізмів безпеки. Міжнародний стандарт ISO 15408, відомий як "Загальні критерії", включає багатофункціональний набір сервісів безпеки, які можуть бути використані як основа для сертифікації.

На адміністративному рівні вкрай важливо сформувати програму робіт у галузі інформаційної безпеки, виділивши необхідні ресурси і забезпечивши контроль за її виконанням. Політика безпеки, яка відображає підхід організації до захисту своїх інформаційних активів, є основою програми. Розробка політики і програми безпеки розпочинається з аналізу ризиків, що передбачає виявлення найпоширеніших загроз.

Серед головних загроз слід відзначити внутрішню складність інформаційних систем, неумисні помилки персоналу та крадіжки. Крім того, аварії підтримувальної інфраструктури, такі як пожежі, можуть становити реальну небезпеку. Хоча зовнішні атаки зростають у кількості, основний збиток все ще завдають внутрішні порушники.

Більшість організацій можуть задовольнитись загальним розумінням ризиків і використовувати типові рішення для забезпечення базового рівня безпеки. Британський стандарт BS 7799:1995, який пропонує типовий каркас, може бути корисним при розробці політики і програми безпеки. Розробка цих документів може бути структурована на кілька рівнів, які відображають різні рівні деталізації. Карта інформаційних систем є важливою складовою програми і політики безпеки, і її треба постійно оновлювати.

Ефективний та економічний захист інформаційних систем (ІС) вимагає ретельного розгляду їх життєвого циклу та впровадження заходів безпеки на кожному етапі. Життєвий цикл ІС складається з кількох фаз, включаючи ініціацію, закупівлю, установку, експлуатацію та виведення з експлуатації. Безпеку не можна просто "прикріпити" до системи; її необхідно враховувати від самого початку і забезпечувати на протязі всього циклу.

На процедурному рівні заходи безпеки спрямовані на людей, а не тільки на технічні аспекти, і охоплюють такі аспекти, як управління персоналом, фізичний

захист, забезпечення працездатності, реагування на порушення безпеки та планування відновних робіт. Важливими принципами безпеки на цьому рівні є безперервність захисту в просторі та часі, розділення обов'язків та мінімізація привілеїв.

Об'єктний підхід та концепція життєвого циклу також мають велике значення на цьому рівні. Об'єктний підхід дозволяє розглядати керовані сутності (наприклад, територію, апаратні засоби тощо) як відносно незалежні підоб'єкти з різним рівнем деталізації та керувати зв'язками між ними.

Розуміння цих принципів та їх впровадження на різних етапах життєвого циклу ІС є надзвичайно важливими для створення надійного та ефективного захисту інформації. Цей підхід допоможе побудувати і зберегти безпечну та надійну систему протягом усього періоду її існування.

Реалізація концепції життєвого циклу відіграє важливу роль як у випадку інформаційних систем, так і у відношенні співробітників. Початковий етап, а саме етап ініціації, передбачає докладне визначення посади, включаючи вимоги до кваліфікації та комп'ютерних привілеїв.

Установчий етап включає проведення навчання, зокрема з урахуванням аспектів безпеки. Через весь період використання необхідно враховувати ризики, пов'язані з недобросовісними співробітниками, та вживати заходів для їх запобігання.

Значна частина успіху в галузі інформаційної безпеки залежить від уважного проведення поточних робіт, включаючи підтримку користувачів, підтримку програмного забезпечення, управління конфігураціями, створення резервних копій, управління носіями, документування та регулярні роботи.

Окрім цього, важливо активно відслідковувати інформацію, що стосується інформаційної безпеки, включаючи підписку на розсилки, які повідомляють про нові загрози, і своєчасно ознайомлюватися з отриманою інформацією.

Також необхідно завчасно готуватися до надзвичайних ситуацій та порушень інформаційної безпеки. Заздалегідь продумана реакція на такі події

спрямована на локалізацію інциденту, мінімізацію завданої шкоди, виявлення порушника та запобігання подальшим порушенням.

Ідентифікація порушника може бути складним процесом, проте планування локалізації інциденту та запобігання повторним порушенням можна виконати з урахуванням всіх деталей.

У разі серйозних аварій необхідне проведення відновних робіт. Процес планування таких робіт передбачає визначення критично важливих функцій організації, ідентифікацію необхідних ресурсів для їх виконання, розпізнавання можливих аварій, розробку стратегії відновних робіт, підготовку до реалізації обраної стратегії та перевірку стратегії перед її застосуванням.

Детальне планування, активне відстеження та готовність до надзвичайних ситуацій сприяють забезпеченню ефективної інформаційної безпеки.

4.1 Технічно-програмні засоби

Програмно-технічні заходи в сфері інформаційної безпеки виконують незамінну роль у контролі комп'ютерних сутностей, таких як обладнання, програми та дані, і є останнім, але надзвичайно важливим шляхом забезпечення безпеки в цифровій сфері. Швидкий прогрес інформаційних технологій приносить як позитивні, так і негативні наслідки. З одного боку, він надає нові можливості для фахівців з інформаційної безпеки, а з іншого боку, зростає складність забезпечення безпеки через постійну модернізацію та використання недостатньо перевірених компонентів, особливо програмного забезпечення.

Забезпечення інформаційної безпеки включає різноманітні види заходів, які працюють у взаємодії для ефективного захисту. Превентивні заходи призначені для запобігання порушенням безпеки та зменшення ризику їх виникнення. Заходи виявлення порушень спрямовані на вчасне виявлення будь-яких порушень безпеки та спроб несанкціонованого доступу. Локалізуючі заходи допомагають обмежити зону впливу порушень та мінімізувати їх наслідки.

Заходи по виявленню порушника спрямовані на ідентифікацію особи, яка здійснює порушення, та забезпечення відповідальності за їхні дії. Заходи відновлення режиму безпеки включають роботи зі відновлення функціонування системи та повернення до нормального режиму після порушення.

При розробці ефективної архітектури безпеки необхідно враховувати всі ці аспекти. Окрім того, важливо дотримуватися певних принципів. Безперервність захисту у просторі та часі означає, що захисні заходи повинні бути постійно активними та непроникними. Використання стандартів та перевірених рішень допомагає забезпечити належну якість захисту. Ієрархічна організація системи допомагає зменшити кількість сутностей на кожному рівні та підвищити стійкість найслабших ланок. Мінімізація привілеїв, розділення обов'язків, ешелонування оборони, використання різноманітних захисних засобів та забезпечення простоти та керованості системи також є важливими аспектами.

Сервіси безпеки охоплюють такі аспекти, як ідентифікація та автентифікація, управління доступом, протоколювання і аудит, шифрування, контроль цілісності, екранування, аналіз захищеності, забезпечення відмовостійкості, безпечне відновлення, тунелювання та управління. Ці сервіси мають бути стійкими до різних загроз, присутніми в різноманітних компонентах та зручними для користувачів і адміністраторів. Наприклад, сучасні засоби ідентифікації та автентифікації повинні бути ефективними у захисті від активного та пасивного прослуховування мережі та забезпечувати безпечний єдиний вхід до системи.

В цілому, забезпечення інформаційної безпеки потребує комплексного підходу, включаючи програмно-технічні заходи, що ретельно плануються та реалізуються з урахуванням всіх аспектів та принципів безпеки. Збільшення обсягу та вдосконалення захисних заходів сприятиме забезпеченню безпеки в умовах швидкого розвитку інформаційних технологій.

Контроль цілісності є важливим аспектом безпеки і може базуватися на криптографічних методах. Введення Закону про електронний цифровий підпис може розширити спектр реалізацій і вирішити проблеми в цій сфері. Однак, на

щастя, існують і не криптографічні підходи до статичної цілісності, які використовують пристрої з одноразовим записом або недоступні для змін. Розділення статичної і динамічної складових системи і збереження статичних даних на незмінних носіях, наприклад, на ПЗП або компакт-диску, може ефективно запобігти загрозам цілісності.

Сервіс екранування є важливою складовою безпеки і має багато потенційних застосувань. Він охоплює не тільки міжмережеві екрани, але й обмеження інтерфейсів та віртуальні локальні мережі. Екрани дозволяють ізолювати та контролювати захищені об'єкти, забезпечуючи високий рівень захищеності і зручність у використанні. Від персональних до корпоративних мереж, використання різних видів міжмережевих екранів і контроль дій зовнішніх та внутрішніх користувачів є розумною практикою.

Аналіз захищеності є інструментом, який підтримує безпеку на протязі життєвого циклу системи. Активний аудит вимагає евристичного підходу, постійного оновлення бази знань та може служити надійним захисним рубежем. Забезпечення відмовостійкості і безпечного відновлення стосується високої доступності системи. Це вимагає включення надмірності в апаратне та програмне забезпечення з урахуванням можливих загроз і зон ураження. Безпечне відновлення є останнім рубежем, який потребує особливої уваги і ретельного проектування, реалізації та супроводу.

Тунелювання є важливим елементом сервісів безпеки, особливо в поєднанні з шифруванням і екрануванням для створення віртуальних приватних мереж.

Управління є необхідним інфраструктурним сервісом для безпечних систем. Система повинна бути керованою, з можливістю моніторингу та прогнозування подій. Використання вільно поширюваних каркасів з поступовим додаванням власних функцій може бути практичним рішенням для багатьох організацій.

4.2 Системи виявлення вторгнень

Один з важливих аспектів безпеки інформації у організації - це виявлення вторгнень. Це активний процес, який здійснюють спеціалісти з безпеки з метою виявлення хакерів і запобігання їх проникненню в систему. Ідеальна система виявлення вторгнень лише сповіщатиме про можливу атаку, не допускаючи незаконного доступу. Цей процес допомагає ідентифікувати активні загрози перед їх реалізацією, надсилаючи оповіщення та попередження про збір інформації зловмисниками, необхідної для атаки. Проте, варто зазначити, що виявлення вторгнень може мати більш складну природу, про що ми розглянемо деталі в подальшому викладі. Перед тим, як глибше вдаватись у деталі виявлення вторгнень, важливо розібратись у сутності цього процесу.

Системи виявлення вторгнень (IDS) існують протягом тривалого часу. Першими прикладами можуть бути нічний дозор і сторожові собаки, які виконували дві важливі функції: виявлення підозрілих дій і обмеження проникнення зловмисників. Часто грабіжники уникали зустрічі з собаками і обходили будівлі, які були захищені цими тваринами. Аналогічно, нічний дозор міг запобігти виявленню злочинців, які не бажали потрапляти під увагу збroєносців чи охоронців, які могли викликати поліцію.

Сигналізаційні системи в будівлях та автомобілях також відносяться до систем виявлення вторгнень. Якщо спрацьовує система оповіщення про підозрілу подію, таку як розбите вікно чи відчинені двері, вона видає сигнал тривоги через включення світлових і звукових сигналів або повідомлення надсилається на пульт поліції. У разі автомобілів, при включеній сигналізації, світиться червона лампочка, що свідчить про активний стан системи.

Усі ці приклади мають спільний принцип - виявлення будь-яких спроб проникнення в захищену зону, таку як офіс, будівля або автомобіль. Визначення периметру захисту в комп'ютерному середовищі виявляється складнішим завданням. У цьому випадку, периметр захисту є віртуальним, і включає комп'ютерні системи, які можуть бути обмежені між мережевими екранами, точками підключення або навіть персональними комп'ютерами з модемами. З

появою бездротових мереж, периметр захисту розширюється до розміру бездротової мережі.

Сигналізація, що сповіщає про проникнення, призначена для виявлення будь-яких спроб незаконного входу в захищену зону, коли ця зона не використовується. IDS-системи, з іншого боку, можна порівняти з охоронцем, який стежить за всім, що відбувається і виявляє недозволені дії, такі як спроба незаконного проникнення чи використання забороненої зброї. У віртуальному світі виявлення таких загроз стає складнішим завданням.

Одним із важливих аспектів є визначення, які події є порушенням безпеки периметра. Наприклад, чи може спроба виявити працюючі комп'ютери бути вважана порушенням? Як слід реагувати на відомі атаки на систему або мережу? Відповіді на ці питання не є простими і залежать від контексту та стану самої системи.

РОЗДІЛ 5. ВПРОВАДЖЕННЯ БАЗОВИХ РЕКОМЕНДАЦІЙ ПО НАЛАШТУВАННЮ БЕЗПЕКИ МЕРЕЖІ НА ПРИКЛАДІ СИМУЛЯЦІЇ PACKET TRACER

Для закріплення матеріалу досліджень впровадимо їх рішення та рекомендації у симуляції корпоративної мережі на основі завдання cisco packet tracer.

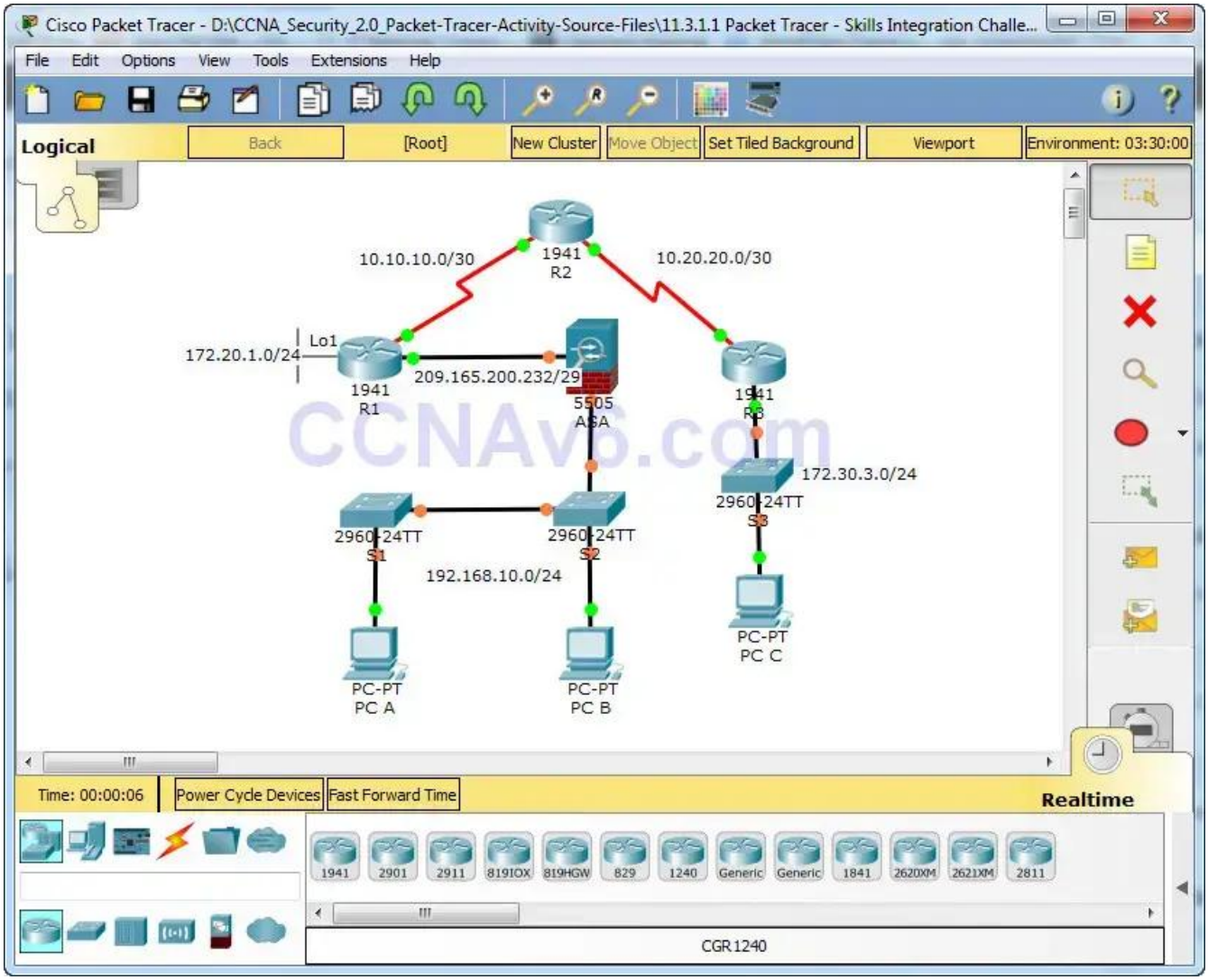

Рисунок 5-1. - Структура мережі-симуляції

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.233	255.255.255.248	N/A
	S0/0/0 (DCE)	10.10.10.1	255.255.255.252	N/A
	Loopback 1	172.20.1.1	255.255.255.0	N/A
R2	S0/0/0	10.10.10.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.20.20.2	255.255.255.252	N/A
R3	G0/1	172.30.3.1	255.255.255.0	N/A
	S0/0/1	10.20.20.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN 1	172.30.3.11	255.255.255.0	172.30.3.1
ASA	VLAN 1 (E0/1)	192.168.10.1	255.255.255.0	N/A
	VLAN 2 (E0/0)	209.165.200.234	255.255.255.248	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	172.30.3.3	255.255.255.0	172.30.3.1

Рисунок 5-2. - Адресна таблиця

Поставлені задачі:

- Налаштувати базову безпеку маршрутизатора
- Налаштувати базовий захист комутатора
- Налаштувати локальну автентифікацію AAA
- Налаштувати SSH
- Захист від атак входу
- Налаштувати міжсайтові IPsec VPN
- Налаштувати параметри брандмауера та IPS
- Налаштуватиосновні параметри безпеки та брандмауера ASA

5.1 Налаштування базової безпеки маршрутизатора

Запити для налаштування маршрутизатора R1:

- Мінімальна довжина пароля становить 10 символів.
- Шифрування паролів відкритого тексту.
- Секретний пароль привілейованого режиму EXEC – ciscoenapa55.
- Пароль рядка консолі – ciscoconpa55, час очікування – 15 хвилин, повідомлення консолі не повинні переривати введення команди.
- Банер із повідомленням дня (MOTD) має містити слово не авторизовано.

Запити для налаштування маршрутизатора R2:

- Секретний пароль привілейованого режиму EXEC – ciscoenapa55.
- Пароль для рядків VTY – ciscovtypa55, час очікування – 15 хвилин, і потрібен вхід.

Для того щоб налаштувати необхідну конфігурацію пристроїв можна скористатись консольним підключенням та використовувати консольні команди

R1:

- conf t
- security passwords min-length 10
- enable secret ciscoenapa55
- service password-encryption
- line console 0
- password ciscoconpa55
- exec-timeout 15 0
- login
- logging synchronous
- banner motd $Unauthorized access strictly prohibited and prosecuted to the full
- extent of the law!$

- end

R2:

- conf t
- enable secret ciscoenapa55
- line vty 0 4
- password ciscovtypa55
- exec-timeout 15 0
- login
- end

5.2 Налаштування базової безпеки комутатора

Завдання:

Запити для налаштування маршрутизатора S1:

- Шифрування паролів відкритого тексту.
- Секретний пароль привілейованого режиму EXEC – ciscoenapa55.
- Пароль консольного рядка – ciscoconpa55, час очікування – 5 хвилин, повідомлення консолі не повинні переривати введення команди.
- Пароль для ліній VTY – ciscovtypa55, час очікування – 5 хвилин, і потрібен вхід.
- Банер MOTD має містити слово неавторизовано.

Налаштований трекінг між S1 і S2 за такими параметрами:

- Встановлення режиму магістралі та призначення VLAN 99 як рідну VLAN.
- Вимкнути генерацію кадрів DTP.

Налаштування S1 за такими параметрами порту:

- F0/6 має дозволити лише режим доступу, встановлений на PortFast і ввімкнути захист BPDU.

- F0/6 використовує базову безпеку порту за замовчуванням із динамічно отриманими MAC-адресами, доданими до поточної конфігурації.
- Усі інші порти мають бути вимкнені.

Команди для базового налаштування комутатора за допомогою консолі:

- conf t
- service password-encryption
- enable secret ciscoenapa55
- line console 0
- password ciscoconpa55
- exec-timeout 5 0
- login
- logging synchronous
- line vty 0 15
- password ciscovtypa55
- exec-timeout 5 0
- login
- banner motd $Unauthorized access strictly prohibited and prosecuted to the full
- extent of the law!$
- end

Налаштування трекінгу між S1 і S2:

- conf t
- interface FastEthernet 0/1
- switchport mode trunk
- switchport trunk native vlan 99
- switchport nonegotiate
- end

Налаштування портів S1:

- conf t
- interface FastEthernet 0/6
- switchport mode access
- spanning-tree portfast
- spanning-tree bpduguard enable
- shutdown
- switchport port-security
- switchport port-security mac-address sticky
- no shutdown
- interface range f0/2 – 5 , f0/7 – 24 , g0/1 - 2
- shutdown
- end

5.3 Налаштування локальної аутентифікації AAA

Завдання:

- Створити локальний обліковий запис користувача Admin01, секретний пароль Admin01pa55 і рівень привілеїв 15.
- Увімкнути служби AAA.
- Впровадити служби AAA, використовуючи локальну базу даних як перший варіант, а потім увімкнути пароль як резервний варіант.

Виконання:

- conf t
- username Admin01 privilege 15 secret Admin01pa55
- aaa new-model
- aaa authentication login default local enable
- end

5.4 Налаштування SSH

Завдання:

- Встановити ім’я домену – ccnasecurity.com
- Ключ RSA має бути згенерований із 1024 модульними бітами.
- Дозволено лише SSH версії 2.
- Тільки SSH дозволено на лініях VTY.

Виконання:

- conf t
- ip domain-name ccnasecurity.com
- crypto key generate rsa
- 1024
- ip ssh version 2
- line vty 0 4
- transport input ssh
- end

5.5 Налаштування захисту від атак на вхід

Завдання:

Налаштувати наступне на R1:

- Якщо користувач не зміг увійти двічі протягом 30 секунд, вимкніть вхід на одну хвилину.
- Записувати всі невдалі спроби входу.

Команди для вирішення:

- conf t
- login block-for 60 attempts 2 within 30
- login on-failure log

5.6 Налаштування міжсайтових IPsec VPN типу "сайт-сайт"

Завдання:

Увімкнути ліцензію на пакет технологій безпеки на R1.

Зберегти поточну конфігурацію перед перезавантаженням.

Налаштувати наступне на R1:

- Створити список доступу, щоб визначити цікавий трафік на R1.
- Налаштувати ACL 101, щоб дозволити трафік від мережі R1 Lo1 до локальної мережі R3 G0/1.

Налаштувати властивості політики шифрування isakmp 10 Phase 1 на R1 і спільний криптоключ ciscovpnpa55. Використовуйте такі параметри:

- Ключовий метод розподілу: ISAKMP
- Шифрування: aes 256
- Хеш: sha
- Метод аутентифікації: попередній доступ
- Обмін ключами: DH Group 5
- Термін служби IKE SA: 3600
- Ключ ISAKMP: ciscovpnpa55

Створити набір трансформацій VPN-SET для використання esp-aes 256 і esp-sha-hmac. Потім створити криптокарту CMAP, яка зв’язує разом усі параметри фази 2. Використати порядковий номер 10 і ідентифікувати його як карту ipsec-isakmp. Використати такі параметри:

- Набір трансформацій: VPN-SET
- Шифрування трансформації: esp-aes 256
- Перетворення автентифікації: esp-sha-hmac
- Ідеальна передня секретність (PFS): група 5
- Назва криптокарти: CMAP
- Встановлення SA: ipsec-isakmp
- Прив’яжіть криптокарту (CMAP) до вихідного інтерфейсу.

Перевірити, чи увімкнено ліцензію пакета Security Technology. Повторити налаштування VPN типу "сайт-сайт" на R3, щоб вони відображали всі конфігурації з R1.

Виконати тестування інтерфейсу Lo1 (172.20.1.1) на R1 із PC-C. На R3 скористатись командою show crypto ipsec sa, щоб переконатися, що кількість пакетів перевищує 0, що означає, що тунель IPsec VPN працює.

Виконання:

Для пристрою R1 застосуємо такі консольні команди:

- conf t
- access-list 101 permit ip 172.20.1.0 0.0.0.255 172.30.3.0 0.0.0.255
- crypto isakmp policy 10
- encryption aes 256
- authentication pre-share
- hash sha
- group 5
- lifetime 3600
- exit
- crypto isakmp key ciscovpnpa55 address 10.20.20.1
- crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
- crypto map CMAP 10 ipsec-isakmp
- set peer 10.20.20.1
- set pfs group5
- set transform-set VPN-SET
- match address 101
- exit
- interface S0/0/0
- crypto map CMAP
- end

Для пристрою R3 застосуємо такі консольні команди:

- conf t
- access-list 101 permit ip 172.30.3.0 0.0.0.255 172.20.1.0 0.0.0.255
- crypto isakmp policy 10
- encryption aes 256
- authentication pre-share
- hash sha
- group 5
- lifetime 3600
- exit
- crypto isakmp key ciscovpnpa55 address 10.10.10.1
- crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
- crypto map CMAP 10 ipsec-isakmp
- set peer 10.10.10.1
- set transform-set VPN-SET
- match address 101
- exit
- interface S0/0/1
- crypto map CMAP
- end

Ці команди налаштовують віртуальну приватну мережу (VPN) між двома пристроями з використанням протоколів ISAKMP і IPsec.

5.7 Налаштування параметрів брандмауера та IPS

Завдання:

Налаштувати ZPF на R3 відповідно до таких вимог:

- Створити зони з назвами IN-ZONE та OUT-ZONE.

- Створити ACL номер 110, який визначає внутрішній трафік, який дозволяє використовувати всі IP-протоколи з вихідної мережі 172.30.3.0/24 до будь-якого пункту призначення.

Створити карту класів під назвою INTERNAL-CLASS-MAP, яка використовує опцію match-all і ACL 110. •

Створити карту політики під назвою IN-2-OUT-PMAP, яка використовує карту класів INTERNAL-CLASS-MAP для перевірки всього відповідного трафіку.

Створити пару зон під назвою IN-2-OUT-ZPAIR, яка визначає IN-ZONE як вихідну зону, а OUT-ZONE як зону призначення.

Вказати, що карта політики IN-2-OUT-PMAP має використовуватися для перевірки трафіку між двома зонами.

Призначити G0/1 як члена IN-ZONE і S0/0/1 як члена OUT-ZONE.

Налаштуйте IPS на R3 відповідно до таких вимог:

- Створити каталог у флеш-пам’яті під назвою ipsdir і встановити його як місце для зберігання підпису IPS.
- Створити правило IPS під назвою IPS-RULE.
- Вилучити категорію всіх підписів із видаленою командою true (усі підписи в межах випуску підпису).
- Вилучити категорію IOS_IPS Basic із видаленою командою false.
- Застосувати вхідне правило до інтерфейсу S0/0/1.

Виконання:

Для пристрою R1 за допомогою консолі вводяться такі команди:

- conf t
- zone security IN-ZONE
- zone security OUT-ZONE
- access-list 110 permit ip 172.30.3.0 0.0.0.255 any
- access-list 110 deny ip any any
- class-map type inspect match-all INTERNAL-CLASS-MAP
- match access-group 110

- exit
- policy-map type inspect IN-2-OUT-PMAP
- class type inspect INTERNAL-CLASS-MAP
- inspect
- zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
- service-policy type inspect IN-2-OUT-PMAP
- exit
- interface g0/1
- zone-member security IN-ZONE
- exit
- interface s0/0/1
- zone-member security OUT-ZONE
- end
- mkdir ipsdir
- conf t
- ip ips config location flash:ipsdir
- ip ips name IPS-RULE
- ip ips signature-category
- category all
- retired true
- exit
- category ios_ips basic
- retired false
- exit
- <Enter>
- interface s0/0/1
- ip ips IPS-RULE in

Ці команди виконують налаштування файрвола та системи запобігання вторгненням для забезпечення безпеки мережі.

5.8 Налаштування основних параметрів безпеки та брандмауера ASA

Завдання:

Налаштувати інтерфейси VLAN з такими параметрами:

- Для інтерфейсу VLAN 1 налаштувати адресацію на використання 192.168.10.1/24.
- Для інтерфейсу VLAN 2 видалити налаштування DHCP за замовчуванням і налаштувати адресацію на використання 209.165.200.234/29.

Налаштувати ім’я хоста, ім’я домену, пароль увімкнення та пароль консолі, використовуючи такі параметри:

- Ім’я хоста ASA – CCNAS-ASA.
- Ім’я домену – ccnasecurity.com.
- Пароль увімкнення режиму – ciscoenapa55.

Створити користувача та налаштувати AAA для використання локальної бази даних для віддаленої автентифікації.

- Налаштувати локальний обліковий запис користувача admin з паролем adminpa55. Не використовувати атрибут encrypted.
- Налаштувати AAA для використання локальної бази даних ASA для автентифікації користувача SSH.
- Дозволити доступ SSH із зовнішнього хосту 172.30.3.3 із тайм-аутом 10 хвилин.

Налаштувати ASA як сервер DHCP, використовуючи такі параметри:

- Призначити IP-адреси внутрішнім клієнтам DHCP від 192.168.10.5 до 192.168.10.30.
- Увімкнути DHCP для прослуховування запитів клієнта DHCP.

Налаштувати статичну маршрутизацію та NAT.

- Створити статичний маршрут за замовчуванням до IP-адреси маршрутизатора наступного переходу (R1).
- Створити мережевий об’єкт під назвою inside-net і призначте йому атрибути за допомогою команд subnet і nat.
- Створити динамічну трансляцію NAT до зовнішнього інтерфейсу.

Змінити Cisco Modular Policy Framework (MPF) на ASA, використовуючи такі налаштування:

- Налаштувати карту класівspection_default відповідно до default-inspection-traffic, а потім вийти у режим глобальної конфігурації.
- Налаштувати список карти політики global_policy. Ввести клас spection_default і ввести команду для перевірки icmp. Потім вийти у режим глобальної конфігурації.
- Налаштувати політику служби MPF, щоб global_policy застосовувалася глобально.

Виконання:

- !CCNAS-ASA
- enable
- <Enter>
- conf t
- interface vlan 1
- nameif inside
- security-level 100
- ip address 192.168.10.1 255.255.255.0
- interface vlan 2
- nameif outside
- security-level 0
- no ip address dhcp
- ip address 209.165.200.234 255.255.255.248

- exit
- hostname CCNAS-ASA
- domain-name ccnasecurity.com
- enable password ciscoenapa55
- username admin password adminpa55
- aaa authentication ssh console LOCAL
- ssh 192.168.10.0 255.255.255.0 inside
- ssh 172.30.3.3 255.255.255.255 outside
- ssh timeout 10
- dhcpd address 192.168.10.5-192.168.10.30 inside
- dhcpd enable inside
- route outside 0.0.0.0 0.0.0.0 209.165.200.233
- object network inside-net
- subnet 192.168.10.0 255.255.255.0
- nat (inside,outside) dynamic interface
- exit
- conf t
- class-map inspection_default
- match default-inspection-traffic
- exit
- policy-map global_policy
- class inspection_default
- inspect icmp
- exit
- service-policy global_policy global

Ці команди налаштовують мережевий пристрій ASA (Adaptive Security Appliance), встановлюють імена, адреси та безпекові рівні для внутрішньої та зовнішньої мереж, налаштовують аутентифікацію SSH та

консолі, налаштовують DHCP-сервер для внутрішньої мережі, встановлюють маршрут за замовчуванням, визначають правила NAT для з'єднання між внутрішньою та зовнішньою мережами, налаштовують інспекцію трафіку ICMP та використовують глобальну політику для цього пристрою.

ВИСНОВКИ

Впровадження комплексної безпеки в корпоративних мережах вимагає проведення аудиту та оцінки поточного стану безпеки мережі. Необхідно виявити потенційні загрози, слабкі місця та ризики, що можуть впливати на мережу. Для цього варто здійснити сканування вразливостей, перевірку конфігурацій обладнання та аналіз потоків даних.

Після оцінки поточного стану безпеки, слід розробити політику безпеки, яка включатиме правила та процедури для захисту мережі. Важливо встановити вимоги щодо паролів, контролю доступу, шифрування даних та резервного копіювання. Крім того, необхідно забезпечити, щоб співробітники були ознайомлені з політикою та дотримувалися її.

Фізична безпека також має велике значення. Для захисту мережевого обладнання та серверних приміщень, слід використовувати контроль доступу до приміщень, відеоспостереження та інші технології.

Для забезпечення безпеки мережі варто використовувати мережеві заходи, такі як фаєрволи, системи виявлення та запобігання вторгнення, віртуальні приватні мережі (VPN) та регулярно оновлювати програмне забезпечення та фірмове забезпечення обладнання.

Для безпеки безпровідних мереж слід застосовувати шифрування, аутентифікацію та інші заходи для запобігання несанкціонованому доступу. Також необхідно використовувати сильні паролі та періодично їх змінювати.

Регулярне резервне копіювання та відновлення даних є важливими для забезпечення безпеки. Всі важливі дані слід резервувати та переконатися, що процедури відновлення працюють належним чином. Резервні копії можна зберігати в захищених приміщеннях або в хмарних сховищах.

Навчання співробітників про загрози безпеки та правила поведінки в мережі є важливим кроком. Регулярні навчання та інформування співробітників допоможуть їм виявляти підозрілу поведінку, фішингові атаки та інші загрози.

Регулярний аудит безпеки мережі дозволяє виявляти нові загрози та слабкі місця. Для цього можна залучати зовнішніх експертів або використовувати спеціалізоване програмне забезпечення для сканування вразливостей та оцінки безпеки мережі.

Важливо розробити план дій в разі виникнення безпекового інциденту, такого як витік даних або кібератака. План має включати процедури повідомлення, відновлення систем та спілкування зі зацікавленими сторонами.

Оновлення та трендів у галузі безпеки мереж є важливим. Використання новітніх технологій та рішень допоможе поліпшити безпеку.

Необхідно враховувати, що кожна організація має свої особливості і потреби, тому варто розробити власну стратегію безпеки, враховуючи ці особливості.

Безпека мережі є не статичним процесом, який вимагає постійного моніторингу, оновлення та покращень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.

2. Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report
https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

3. Руководство по технологиям объединенных сетей. 3-е издание. Пер. с англ. М.: Вильямс, 2002. – 1040 с.

4. Шринивас В. Качество обслуживания в сетях IP / В. Шринивас. – М.: Вильямс, 2003. – 851 с.

5. Mueller S. Upgrading and Repairing Networks / S. Mueller. – Que, 2002.

6. Lekkas P. C. Network Processors / P. C. Lekkas. – The McGraw-Hill Companies, 2003.

7. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.

8. Богуш В. М. Інформаційна безпека від А до Я: 3000 термінів і понять / В. М. Богуш, А. М. Кудін. – К.: МОУ, 1999. – 456 с.

9. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: ООО «ТИД ДС», 2004. – 992 с.

10. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 120 с.

11. Уфимцев Ю. С. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов, Е. А. Ерофеев и др. – М.: Экзамен, 2004. – 544 с.

12. Architecting the Next Generation of OT Cybersecurity:
https://www.ponemon.org/research/ponemon-library/security/architecting-the-next-generation-of-ot-cybersecurity.html