**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**

**імені ІГОРЯ СІКОРСЬКОГО”**

**ЗВІТ**

**з лабораторної роботи №3**

**з навчальної дисципліни “Інформаційне забезпечення безпеки**

**комп’ютерних систем”**

**Тема:**

**Аналіз ризиків та основні принципи забезпечення безпеки**

**Варіант 20**

**Виконав студент групи ТР–12**

Руденко Владислав\_\_\_\_\_\_\_\_\_

Лабораторну роботу захищено

з оцінкою \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ 2024**

**Мета роботи:** ознайомлення та дослідження алгоритму оцінкиризиківінформаційної безпеки організації; набуття практичних навичок щодо застосуванняметодики матричного аналізу ризиків інформаційної безпеки та наданняосновнихрекомендацій з забезпечення безпеки.

**Індивідуальне завдання на лабораторну роботу:**



1. Провести аналіз та оцінку ризиків безпеки організації (згідно варіанту) за допомогою матричного підходу.
2. На основі отриманих результатів, надати основні рекомендації щодозабезпечення безпеки в даній організації.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків безпеки.
4. Сформовані списки та обґрунтування інформаційних активіворганізації,ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.
6. Основні рекомендації щодо забезпечення безпеки в даній організації.
7. Висновки та відповіді на контрольні питання:

* Як класифікуються загрози за результатами їх впливу на інформацію?
* Що таке НСД і які існують способи його реалізації?
* Які повинна вирішувати завдання система забезпечення безпеки комп’ютерної системи? Які існують поширені прийоми НСД?
* Які існують основні категорії мережевих атак?
* У чому полягають принципи управління доступом?
* У чому сенс концепції матриці доступу?
* Що є функціями і механізмами захисту?

1. Оформити звіт до лабораторної роботи.

**Хід виконання роботи**

1. **Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків безпеки.**

**Назва організації:** Інтернет-провайдер "PodPivas"

**Сфера діяльності:** Організація надає послуги доступу до Інтернету для приватних осіб, бізнесу та державних установ. Основними послугами є високошвидкісний Інтернет, технічна підтримка користувачів, оренда серверів та хмарних рішень, а також забезпечення безпеки мережі.

**Основні напрями діяльності:**

1. Забезпечення стабільного та швидкого доступу до мережі Інтернет для користувачів через різні типи підключень (оптоволоконний, кабельний, бездротовий).
2. Зберігання та захист конфіденційної інформації клієнтів, включаючи особисті дані та інформацію про оплату.
3. Підтримка та обслуговування серверного та мережевого обладнання, необхідного для надання послуг Інтернету.
4. Забезпечення кібербезпеки клієнтів шляхом фільтрації небезпечного контенту та захисту від кіберзагроз.

**Інформаційна безпека для Інтернет-провайдера є важливим фактором**, оскільки порушення роботи мережі чи витік даних можуть призвести до фінансових втрат, втрати довіри клієнтів та юридичних наслідків.

**Ключові цілі забезпечення інформаційної безпеки:**

1. **Захист конфіденційності даних клієнтів** – запобігання несанкціонованому доступу до особистої та платіжної інформації користувачів.
2. **Гарантія доступності мережевих послуг** – забезпечення безперебійного доступу клієнтів до Інтернету, попередження та протидія DDoS-атакам.
3. **Підтримка цілісності даних та обладнання** – захист систем від пошкоджень або зловмисних втручань, зокрема захист серверів та мережевих пристроїв від шкідливого програмного забезпечення й атак на обладнання.

**2. Сформовані списки**

### 2.1 Інформаційні активи

Інформаційні активи, визначені в рамках аналізу ризиків, включають:

1. **Дані клієнтів.** Включають особисту інформацію та історію платежів користувачів, зберігання яких має бути захищене відповідно до нормативних вимог.
2. **Мережеве обладнання.** Сервери, маршрутизатори, комутатори, які забезпечують надання послуг доступу до Інтернету для клієнтів.
3. **Системи управління мережами (NMS).** Платформи, що дозволяють адмініструвати, моніторити та налаштовувати обладнання й мережу.
4. **Веб-платформа клієнтської підтримки.** Портал, через який клієнти можуть залишати запити, отримувати підтримку та доступ до інформації про обслуговування.

### 2.2 Уразливості

Визначено такі уразливості, що можуть впливати на інформаційні активи Інтернет-провайдера:

1. **Вразливість мережевого обладнання.** Неправильна конфігурація маршрутизаторів та комутаторів може дозволити несанкціонований доступ до мережі.
2. **Недостатнє навчання персоналу.** Людський фактор може призвести до помилок при роботі з критичними системами та даними клієнтів.
3. **Недостатній захист веб-платформи клієнтської підтримки.** Платформа може бути піддана атакам типу SQL-ін'єкцій та XSS-атак.
4. **Використання слабких паролів.** Недостатній контроль за паролями співробітників може полегшити злом систем аутентифікації.
5. **Неправильне налаштування систем управління мережами.** Це може дозволити несанкціонований доступ до адміністрування мережі.

### 2.3 Загрози

На основі виявлених уразливостей визначені основні загрози:

1. **Несанкціонований доступ до мережі.** Може призвести до витоку даних клієнтів або зниження якості послуг.
2. **DDoS-атаки.** Можуть паралізувати роботу мережі та обмежити доступ клієнтів до Інтернету.
3. **Шкідливе програмне забезпечення.** Наприклад, програми-вимагачі, які можуть заблокувати доступ до критичних систем або даних.
4. **Фішингові атаки.** Мета — викрасти облікові дані співробітників або клієнтів для подальшого доступу до систем провайдера.
5. **Збої в роботі мережевого обладнання.** Можуть спричинити збої в наданні послуг та зниження якості обслуговування.

### 2.4 Засоби контролю

Рекомендовані засоби для мінімізації ризиків:

1. **Міжмережевий екран (Firewall).** Захищає мережу провайдера від зовнішніх атак.
2. **Системи виявлення та запобігання вторгнень (IDS/IPS).** Допомагають ідентифікувати й блокувати підозрілу активність.
3. **Навчання персоналу.** Підвищує обізнаність працівників щодо загроз кібербезпеки та методів їх уникнення.
4. **Мультифакторна автентифікація (MFA).** Посилює захист облікових записів співробітників.
5. **Резервне копіювання даних.** Забезпечує доступність критичних даних і систем у разі збоїв або атак.
6. **Моніторинг мережі.** Регулярний моніторинг допомагає швидко виявляти аномалії у трафіку та потенційні загрози.

**3. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.**

**Матриця Уразливостей:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Активи:** | Персональні дані клієнтів | Персональні Комп'ютери | Веб-платформа | Мережеве обладнання | Всього | Ранжуванння |
| **Уразливості** | РП | 4 | 3 | 2 | 1 | **Σ** |  |
| Неправильна конфігурація мережевого обладнання | 2 | 1 | 1 | 2 | 4 | 15 | 1 |
| Відсутність оновлень ПЗ | 4 | 0 | 8 | 2 | 5 | 33 | 3 |
| Недостатній контроль доступу | 3 | 8 | 7 | 8 | 3 | 72 | 4 |
| Слабкі паролі | 5 | 9 | 9 | 7 | 5 | 82 | 5 |
| Відсутність резервного копіювання даних | 1 | 4 | 0 | 4 | 2 | 26 | 2 |

Матриця уразливостей демонструє, що найбільші ризики пов'язані з недоліками в конфігурації мережевих компонентів, а також у відсутності систематичного оновлення програмного забезпечення. Відсутність оновлень робить системи вразливими до відомих загроз і значно підвищує ризик зовнішніх атак. Недостатній контроль доступу та слабкі паролі також відіграють ключову роль у посиленні вразливості. Якщо працівники мають доступ до конфіденційних даних, але при цьому не дотримуються суворих вимог до захисту облікових записів, це створює додаткові ризики для безпеки інформації. Резервне копіювання даних є важливим компонентом стійкості системи, і його відсутність вказує на високий рівень ризику у разі непередбачуваних інцидентів, таких як вірусні атаки або технічні збої. Матриця показує, що організація повинна приділити увагу базовим заходам захисту та оновлення систем, щоб уникнути експлуатації цих уразливостей.

**Матриця Загроз:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Активи:** | Доступ до мережі | Конфіденційні дані клієнтів | Обладнання (сервери, роутери) | Програмне забезпечення | Всього | Ранжуванння |
| **Загроз** | РП | 4 | 3 | 2 | 1 | **Σ** |  |
| Відмова в обслуговуванні (DoS) | 5 | 5 | 1 | 2 | 4 | 31 | 2 |
| Шкідливе програмне забезпечення | 4 | 3 | 8 | 5 | 5 | 51 | 3 |
| Атаки на обладнання | 3 | 3 | 7 | 5 | 9 | 52 | 4 |
| Фішинг | 2 | 2 | 9 | 7 | 5 | 54 | 5 |
| Необережність працівників | 2 | 4 | 3 | 0 | 4 | 29 | 1 |

Аналіз матриці загроз свідчить про те, що організація стикається з різноманітними потенційними загрозами, включаючи відмову в обслуговуванні (DoS-атаки), шкідливе програмне забезпечення, атаки на обладнання, фішинг та людський фактор. Найбільшу загрозу становить шкідливе програмне забезпечення та атаки на обладнання, які можуть мати серйозний вплив на цілісність, конфіденційність та доступність даних. Відмова в обслуговуванні вказує на можливість втрати доступності для користувачів, що впливає на безперервність бізнес-процесів. Фішингові атаки та недбалість персоналу є основними загрозами, пов’язаними з людським фактором, що підкреслює важливість навчання працівників. Загалом, матриця загроз свідчить про те, що організація повинна зосередити свої зусилля не лише на технічних засобах захисту, але й на розвитку інформаційної культури серед співробітників, щоб зменшити вплив людського фактору на безпеку.

**Матриця контролю:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Активи:** | Персональні дані клієнтів | Персональні Комп'ютери | Веб-платформа | Мережеве обладнання | Всього | Ранжуванння |
| **Контроль** | РП | 4 | 3 | 2 | 1 | **Σ** |  |
| Міжмережевий екран (Firewall) | 5 | 2 | 9 | 7 | 8 | 57 | 3 |
| Регулярне оновлення ПЗ та патчів | 3 | 1 | 3 | 7 | 9 | 36 | 2 |
| Багатофакторна автентифікація (MFA) | 4 | 7 | 8 | 4 | 8 | 68 | 5 |
| Політика управління паролями | 3 | 6 | 7 | 4 | 8 | 61 | 4 |
| Система моніторингу та аудиту | 2 | 2 | 3 | 2 | 5 | 26 | 1 |

Матриця контролю підтверджує, що для зниження ризиків доцільно використовувати різні підходи до безпеки, зокрема, фаєрволи, багатофакторну автентифікацію, регулярне оновлення програмного забезпечення, управління паролями та моніторинг системи. Найефективнішим засобом контролю виявляється багатофакторна автентифікація, яка значно ускладнює можливість отримання доступу до важливих систем без належного рівня авторизації. Крім того, використання фаєрволів та політики управління паролями підвищує загальну безпеку мережі, знижуючи можливість несанкціонованого доступу. Регулярне оновлення програмного забезпечення та застосування патчів знижує ризик експлуатації відомих вразливостей у системах. Система моніторингу і аудиту є менш ефективною порівняно з іншими заходами, але забезпечує важливий рівень спостереження, дозволяючи виявляти потенційні загрози на ранній стадії. Загалом, матриця показує необхідність інтеграції різних засобів контролю для забезпечення комплексного захисту активів.

**4. Основні рекомендації щодо забезпечення безпеки в даній організації.**

**1.Коректна конфігурація мережевого обладнання:**

* **Провести аудит налаштувань мережевого обладнання** (маршрутизатори, комутатори) для виявлення можливих вразливостей.
* **Впровадити політику мінімального доступу** – обмежувати доступ до критичних систем лише для авторизованих користувачів.
* **Оновлювати прошивку та сигнатури безпеки обладнання** для захисту від нових загроз.
* **Налаштувати журналювання подій (logging)** для моніторингу активності та виявлення підозрілих дій.
* **Регулярно перевіряти та тестувати** правила брандмауерів і фільтрації трафіку для мінімізації ризиків.

**2.Підвищення обізнаності персоналу щодо кібербезпеки:**

* **Розробити програму навчання з кібербезпеки** для працівників, яка включатиме теми, такі як розпізнавання фішингових атак, основи захисту даних, соціальна інженерія.
* **Проводити практичні вправи та симуляції** – наприклад, симуляцію фішингових атак для підвищення обізнаності персоналу.
* **Організувати регулярні перевірки знань** з кібербезпеки для перевірки рівня підготовки співробітників.
* **Оновлювати навчальні матеріали відповідно до нових загроз**, щоб персонал міг вчасно реагувати на потенційні атаки.
* **Заохочувати повідомлення про підозрілу активність** через визначені процедури.

**3.Використання систем моніторингу та виявлення загроз:**

* **Впровадити IDS/IPS (системи виявлення та запобігання вторгненням)** для моніторингу мережевого трафіку та виявлення підозрілої активності.
* **Налаштувати SIEM (Security Information and Event Management)** для збору та аналізу даних безпеки з різних джерел.
* **Регулярно перевіряти журнали активності** для виявлення можливих порушень і потенційних атак.
* **Налаштувати автоматичні сповіщення про підозрілу активність** для оперативного реагування на загрози.
* **Проводити періодичні перевірки мережі** та оцінки безпеки, щоб виявляти нові вразливості.

**4.Резервне копіювання даних:**

* **Налаштувати автоматичне резервне копіювання критичних даних** у кількох географічних локаціях для забезпечення доступності.
* **Забезпечити шифрування резервних копій** для захисту конфіденційної інформації клієнтів і системних даних.
* **Регулярно перевіряти цілісність та доступність резервних копій** для відновлення.
* **Зберігати резервні копії в онлайн- і офлайн-середовищах** для більшої стійкості до атак і збоїв.
* **Розробити та протестувати план відновлення даних (Disaster Recovery Plan)** для швидкого відновлення роботи після інциденту.

**5.Багатофакторна автентифікація (MFA):**

* **Впровадити багатофакторну автентифікацію для всіх критичних систем** і облікових записів, зокрема для адміністраторів та співробітників.
* **Забезпечити використання кількох рівнів перевірки,** таких як паролі, біометрія або одноразові коди (OTP).
* **Періодично оновлювати алгоритми та інструменти MFA** для захисту від нових методів злому.
* **Інтегрувати MFA із загальною системою безпеки** для створення багаторівневого захисту.
* **Навчати персонал про важливість MFA** та інформувати про правила використання.

**6.Регулярний аудит та оновлення політик безпеки:**

* **Проводити регулярний аудит безпеки** для ідентифікації слабких місць у системах та процедурах.
* **Оновлювати політики безпеки відповідно до нових вимог** і нормативних актів.
* **Розробити процедури реагування на інциденти,** які включатимуть детальний опис кроків реагування, щоб мінімізувати шкоду у разі атаки.
* **Створити резервну документацію та протоколи дій** для забезпечення готовності до різних кіберзагроз і технологічних збоїв.

**5. Висновок:**

У ході виконання лабораторної роботи було проведено аналіз основних загроз інформаційній безпеці в організації Інтернет-провайдера. Було визначено ключові інформаційні активи, такі як мережеве обладнання, персональні дані клієнтів, системи управління та веб-платформа обслуговування клієнтів. Для кожного з активів було ідентифіковано можливі вразливості та потенційні загрози, які можуть призвести до втрати конфіденційності, цілісності та доступності даних.

Розроблений набір рекомендацій включає заходи для підвищення безпеки, такі як коректна конфігурація мережевого обладнання, навчання персоналу з питань кібербезпеки, використання систем моніторингу, резервне копіювання даних та багатофакторна автентифікація. Впровадження цих заходів допоможе зменшити ризик кіберзагроз та підвищити загальний рівень захищеності інформаційних активів організації.

**6. Відповіді на Запитання:**

1. **Як класифікуються загрози за результатами їх впливу на інформацію?**

- **Конфіденційність:** Ризик ненавмисного розкриття інформації, наприклад, через фішинг чи витоки даних.

- **Цілісність:** Ризик несанкціонованого внесення змін у дані сторонніми, наприклад, через шкідливе ПЗ, що модифікує або псує інформацію.

- **Доступність:** Порушення доступу до інформації або сервісів, наприклад, в результаті DDoS-атак.

2. **Що таке НСД і які існують способи його реалізації?**

- Ризик доступу до конфіденційних даних без дозволу.

- Використовувані методи:

- **Фізичний доступ:** Використання слабких фізичних заходів безпеки.

- **Програмний доступ:** Експлуатація вразливостей у програмному забезпеченні.

- **Соціальна інженерія:** Маніпулювання співробітниками для отримання доступу.

3. **Які повинна вирішувати завдання система забезпечення безпеки комп’ютерної системи?**

- **Захист даних:** Запобігання знищенню, витоку чи зміні інформації.

- **Моніторинг:** Спостереження і аналіз активності для виявлення загроз.

- **Управління доступом:** Надання прав доступу тільки авторизованим особам.

4. **Які існують поширені прийоми НСД?**

- **Фішинг:** Обман користувачів з метою отримання їхніх облікових даних.

- **Перехоплення даних:** Використання шкідливих пристроїв або ПЗ для збору даних.

- **Експлуатація вразливостей:** Використання слабких місць у ПЗ або налаштуваннях.

5. **Які існують основні категорії мережевих атак?**

- **DDoS-атака:** Перевантаження сервера, що призводить до його відмови у наданні послуг.

- **MITM** (Атака посередника): Перехоплення даних між двома сторонами.

- **SQL-ін'єкція**: Введення шкідливих SQL-запитів через веб-форми для отримання доступу до баз даних.

6. **У чому полягають принципи управління доступом?**

- **Мінімізація привілеїв:** Надання доступу лише до необхідних функцій.

- **Розподіл обов’язків:** Запобігання зловживанням через розподіл прав.

- **Принцип необхідності знати:** Доступ надається лише до тих даних, що потрібні для виконання роботи.

7. **У чому сенс концепції матриці доступу?**

- Інструмент для наочного відображення прав доступу.

- Вказує, які користувачі мають доступ до конкретних ресурсів і на якому рівні.

8. **Що є функціями і механізмами захисту?**

- **Шифрування**: Захист інформації через її кодування.

- **Аутентифікація**: Перевірка особистості користувача.

- **Антивірус**: Захист системи від шкідливого ПЗ.

- **Моніторинг**: Постійне відстеження для виявлення підозрілої активності в реальному часі.