УДК 62-523.8

ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ПРИНЦИПІВ РЕАЛІЗАЦІЇ ЗАХОДІВ БЕЗПЕКИ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Бистрик С.Л. – гр.МгІТ2-24, bsl_1@ukr.net
Яхно В.М. – к.т.н., ст. викладач, yaxno.vm@knutd.edu.ua
Київський національний університет технологій та дизайну

Мета роботи – побудова безпечної комп’ютерної мережі підприємства.

Одна із важливих проблем комп’ютерної мережі підприємства це безпека. В залежності від обсягів та типів інформації, що циркулює в мережі існує декілька важливих напрямків забезпечення захисту електронної інформації в комп'ютерній мережі підприємства. Для ефективного розв’язання проблеми безпеки вони повинні застосовуватися комплексно.

Перший напрямок стосується документальних, процедурних та кадрових заходів, які регламентують використання інформаційних ресурсів та відповідальність персоналу. Необхідними складовими є:

1. Розробка політики безпеки інформації (ПБІ): Створення внутрішніх нормативних документів, що чітко визначають правила, процедури, права та обов'язки співробітників щодо роботи з конфіденційною інформацією та ресурсами мережі;

2. Система управління доступом: Встановлення чітких правил ідентифікації, автентифікації та авторизації користувачів (наприклад, складні паролі, багатофакторна автентифікація (MFA), принцип найменших привілеїв).

3. Стандартний регламент реагування на інциденти: Розробка планів дій на випадок виявлення порушень безпеки, вторгнень чи збоїв, включаючи процедури відновлення даних та розслідування.

4. Контроль фізичного доступу: Обмеження доступу до серверних приміщень, мережевого обладнання та носіїв інформації.

Наступний важливий напрямок – це використання спеціальних технічних засобів і програмного забезпечення для безпосереднього запобігання, виявлення та протидії загрозам.

Важливим компонентом напрямку є мережевий захист, що потребує розподілу мережі на логічні сегменти. Цю технологія може бути енергозберігаючою і її забезпечують наступні засоби [1-2]:

- Міжмережеві екрани (Firewalls): Фільтрація мережевого трафіку між корпоративною мережею та зовнішніми мережами (наприклад, Інтернетом) або між сегментами внутрішньої мережі (мережева сегментація).

- Системи виявлення та запобігання вторгненням (IDS/IPS): Моніторинг мережевого трафіку для виявлення підозрілої активності та блокування потенційних атак.

- VPN (Virtual Private Network): Створення захищених (зашифрованих) каналів зв'язку для віддалених співробітників або між офісами через незахищені мережі (Інтернет).

- Безпечна конфігурація обладнання: Налаштування маршрутизаторів, комутаторів та інших пристроїв з урахуванням мінімальних необхідних сервісів та максимального рівня захисту.

Наступний важливий напрямок – це захист кінцевих пристроїв та даних. Ця проблема потребує впровадження наступних організаційних та програмних засобів.

- Антивірусний та анти шкідливий захист: Використання програм для виявлення, блокування та видалення шкідливого програмного забезпечення (віруси, трояни, програми-вимагачі).

- Системи контролю доступу: Програмні засоби для розмежування прав доступу до файлів, тек, баз даних на рівні операційної системи та прикладного ПЗ.

- Резервне копіювання (Backup): Регулярне створення копій критично важливої інформації та тестування процедур відновлення для забезпечення доступності даних.

- Управління оновленнями (Patch Management): Своєчасне встановлення оновлень операційних систем та програмного забезпечення для усунення вразливостей.

Для комплексного розв’язання проблеми і застосування наведених механізмів необхідно узгодження рішень всіх важливих користувачів мережі. Навіть термін важливий користувач є недостатньо визначеним. Невизначеність виникає тому що особа (особи), що приймає рішення, не має достатньої інформації про можливі стани зовнішнього середовища (події, що не залежать від її дій) або не може визначити ймовірність настання цих станів.

Висновки. Прийняття рішень до засобів безпеки в умовах невизначеності вимагає застосування спеціальних методів, які допомагають обрати найкращий варіант дій, коли ймовірності майбутніх подій невідомі або їх неможливо точно оцінити.

Цей процес базується на системному аналізі та врахуванні різних критеріїв оцінки ризику.

Список використаних джерел:

1. Мережеве обладнання [Електронний ресурс] // Режим доступу: https://mikrotik.com/

2. Microsoft [Електронний ресурс] // Режим доступу: https://learn.microsoft.com/