кого ступеня очищення забрудненого повітря шляхом прискорення тангенціального руху його в пиловловлюючій воронці та збільшення дії відцентрових сил на пилові частки; уникнути втрат матеріалу при аспірації. Крім того, очищення повітря всередині аспіраційного укриття полегшує і здешевлює процес очищенняаспіраційного повітря в пиловловлювачах на наступних ступенях очистки. При цьому, підвищується надійність експлуатації мережі трубопроводів системи аспірації, знижується ймовірність відкладення пилу в трубопроводах на горизонтальних і похилих ділянках мережі, зменшується абразивне зношення стінок трубопроводів, що підвищує в цілому ефективність роботи системи аспірації.

Список літератури

1.Обеспечение эффективных рабочих режимов аспирационных систем фабрик окомкования ГОКов в условиях длительной эксплуатации / **А.М. Голышев, С.И. Задорожний, А.В. Герасимчук, А.А. Голышев** // Разработка рудных месторождений. – КривийРіг, 2007. – Вип. 91. – С. 232-236.

2. **Деньгуб Т.В.** Исследование аэродинамического сопротивления аспирационных воздуховодов при пылевых отложениях / **Т.В. Деньгуб, Н.В. Худик** // Металлургическая и горнорудная промышленность. – Днепропетровск, 2014. – № 4. – С. 115-117.

3. А. с. 947015 СССР, МПК В 65 G 21/00. Укрытие места загрузки ленточного конвейера / **Н.Ф. Гращенков, В.С. Харьковский, Б. Цай** и др. – №2874795/27-03; заявл. 24.01.80 опубл. 30.07.82, Бюл. №28.

4. Патент на изобретение №2071568 Российская Федерация, МПК E21F5/00, B65G21/00. Аспирационное укрытие места перегрузки сыпучего материала, подаваемого на ленточный конвейер / **В.П. Наумов, Б.Г. Моргун, В.А. Минко** и др.; заявитель и правообладатель Белгород.гос. технол. академия строит. материалов. – №95103028/03; заявл. 02.03.1995; опубл. 10.01.1997, бюл. №1.

5.А. с. 1449495 СССР, МПК B65G69/18, 65/30. Устройство для перегрузки сыпучего материала / **И.Н. Логачев, Л.М. Черненко, Г.В. Слюсаренко**. - №4191745/23-11; заявл. 11.02.1987; опубл. 07.01.1989; бюл. №1.

6. Патент на корисну модель № 52371. Україна. МПК Е 21 F 5/00, В 08 В 15/00. Аспіраційнеукриттявузлівперевантаження сипких матеріалів. / **Лапшин О.Є, Немченко А.А., Шаповалов В.А., Філонов В.А., Худик М.В.**; заявник і власникКриворізькийтехнічний університет. – № u201001807; заявл. 19.02.2010; опубл. 25.08.2010. Бюл. № 16.

7. **Феськов М.И.** Использование факелов диспергированной воды для пылеотсоса / **М.И. Феськов** // Безопасность труда в промышленности. – 1982. – №9. – С. 44-46.

8. **Лапшин О.Є.** Поліпшення ефективності роботи аспіраційних укриттів перевантажувальних вузлів / **О.Є. Лапшин, А.А. Немченко, В.А. Коновалюк, О.О. Лапшин, М.В. Худик** // Вісник Криворізького технічного університету: зб. наук. праць. – Кривий Ріг, 2012. – Вип. 31. – С. 285-289.

9. Пылеулавливание в металлургии / [**Алешина В.М., Вальдберг А.Ю., Гордон Г.М.** и др.]; под ред. **А.А. Гурвица**. – М.: Металлургия, 1984. – 336 с.

10. Патент на корисну модель. Аспіраційне укриття вузла перевантаження стрічкового конвеєра. / **Лапшин О.Є, Лапшин О.О., Шаповалов В.А., Лапшина Д.О.**; заявник і власник Криворізький технічний університет. – № u201709932; заявл. 13.10.2017.

Подано до редакції 20.03.2018

УДК 004.056.52:334.78

Н.О. КАРАБУТ, ст. викладач, Д.В. ШВЕЦЬ, асистент, Криворізький національний університет

ЗАСОБИ ПІДВИЩЕННЯ БЕЗПЕКИ ДАНИХ В КОРПОРАТИВНИХ МЕРЕЖАХ

Мета. Метою даної роботи є аналіз існуючих засобів підвищення безпеки даних в корпоративних мережах та виявлення найбільш вразливих ланок в програмному та апаратному забезпеченні, що можуть нести загрозу безпеці даних в корпоративній мережі та її функціонуванню в умовах можливих хакерських атак.

Методи дослідження. Розглянуто існуючі засоби організації корпоративних мереж та виявлено методи підвищення безпеки передачі та збереження даних, що поділяються на керування правами сервісних облікових записів, керування доступом до мережевих ресурсів та способами підключення до них, використання демілітаризованої зони, сегментацію мережі, шифрування трафіку та налаштування віддаленого доступу. Розглянуто можливі налаштування операційних систем та програмних засобів, які можуть ускладнити процес вторгнення в систему, що захищається. Звернута увага на налаштування, які можуть понизити рівень безпеки або поставити під загрозу приватність інформації в корпоративній мережі.

Наукова новизна. Розв'язання даної задачі складає актуальність роботи. Її метою є аналіз методів захисту даних в корпоративних мережах, що існують на сьогоднішній день, їх класифікація, розгляд технологічних особливостей реалізації, та подальша розробка нових методів підвищення безпеки зберігання та передачі даних в корпоративних мережах.

Практична значимість. Проаналізовано низку можливих варіантів вирішення проблеми безпеки даних в корпоративних мережах та засобів унеможливлення атак зловмисників на інформаційні системи, зазначено способи їх використання та особливості налаштувань. Аналіз існуючих методів, їх переваг та недоліків, дозволить розробити нові методи підвищення рівня безпеки корпоративних мереж при їх застосуванні.

Результати. Розглянуті програмні та апаратні засоби забезпечення належного рівня безпеки корпоративних мереж дозволяють зменшити ризик атаки на інформаційну систему, що захищається, та їх аналіз дозволить в подальшому синтезувати нові методи підвищення безпеки зберігання та передачі даних в корпоративних мережах та покращення їх протидії зовнішнім атакам.

Ключові слова: корпоративні мережі, безпека, захист даних.

doi: 10.31721/2306-5451-2018-1-46-122-126

Проблема та її зв'язок з науковими та практичними завданнями. Фактори IT-безпеки корпоративних мереж постійно змінюються під впливом хмарних обчислень, проникнення IT-технологій у життя користувачів і інтенсифікації робочого часу. Кожен сервер в корпоративній мережі є потенційною мішенню для кібератаки в силу ряду причин (наявності відкритих портів для встановлення з'єднань, відсутності необхідних патчів, можливої відсутності моніторингу активності). У зв'язку з цим особам, які приймають рішення в сфері інформаційних технологій та інформаційної безпеки, доводиться знаходити тонкий баланс між дотриманням безпеки корпоративних даних і збереженням простоти, доступності і зручності в експлуатації, яких очікують користувачі.

Аналіз досліджень і публікацій. В джерелах [1-10] розглянуто низку засобів підвищення безпеки в корпоративних мережах і методів, спрямованих на забезпечення захисту передачі інформації в корпоративних каналах. Тим не менш, в більшості випадків описані рішення можуть бути застарілими в зв'язку з розвитком програмних та апаратних засобів і не забезпечувати належний рівень захисту. Дана робота є намаганням класифікувати існуючі актуальні методи підвищення безпеки корпоративних мереж та засоби перевірки їх рівня безпеки.

Постановка завдання. Розглянути можливі методи та засоби підвищення безпеки передачі даних в корпоративних мережах та збереження інформації від несанкціонованого доступу та модифікації.

Викладення матеріалу та результати. При використанні операційних систем Windows актуальним завданням є посилення безпеки інфраструктури системи за допомогою ряду методів:

Деталізація прав сервісних облікових записів. Облікові записи Windows мають набір різних прав входу в систему. Це локальний вхід, вхід в якості пакетного завдання, в якості служби, та ін. У великому домені завжди є службові облікові записи, які необхідні для масової роботи різного ПЗ, служб, запуску завдань, і т.д. Для підвищення безпеки необхідно мінімізувати права даних облікових записів під свою область застосування, і явно заборонити непотрібні повноваження. Це знизить ризики швидкого поширення загроз у разі втрати контролю над таким записом.

У корпоративній мережі доцільно створювати окремі облікові записи:

для роботи зі своєю особистою машиною;

для входу на контролери домену та управлінням ними;

для серверів;

для робочих станцій;

для віддалених філій;

для зони DMZ.

Використання UAC. UAC (User Account Control, UAC) є компонентом безпеки в операційних системах Windows. UAC дозволяє користувачам виконувати спільні завдання без прав адміністратора і з правами адміністратора без необхідності перемикання між обліковими записами, виходу з системи або використання опції «Запуск від імені».

Використання UAC є нагально рекомендованим, причому на найбільш високому рівні безпеки. Обійти UAC або підвищити права цілком можливо, однак це є додатковою перешкодою для зловмисника.

Відключення прихованих файлових ресурсів. Спільні файлові ресурси (shares) призначені для надання віддаленого доступу до файлів. За замовчуванням в Windows можуть бути створені приховані адміністративні загальні ресурси, до яких можуть підключатися користувачі локальної мережі:

кореневі розділи або тома C$ (D$ E$ F$ і т. д.);

загальний ресурс ADMIN$ - кореневий каталог операційної системи (%SYSTEMROOT%), в якому встановлена операційна система Windows;

загальний ресурс IPC$ - для організації тимчасових зв'язків, що створюються додатками для обміну даними з допомогою іменованих каналів (як правило, застосовується для віддаленого адміністрування серверів в мережі);

загальний ресурс PRINT$ - для віддаленого адміністрування принтерів;

загальний ресурс FAX$ - для віддаленого адміністрування факсів.

Вище перераховані адміністративні ресурси, доступ до яких мають лише члени групи локальних адміністраторів на комп'ютері. За наявності адміністраторських привілеїв можна отримати необмежений доступ до файлової системи на віддаленому комп'ютері. Ситуація часто ускладнюється тим, що обліковий запис адміністратора може бути не захищений паролем і будь-який користувач, незалежно від рівня привілеїв, зможе використовувати ресурс.

Адміністративні ресурси дуже зручні в плані адміністрування, але з точки зору безпеки вони є додатковою вразливістю. Для відключення загальних файлових ресурсів необхідно відключити відповідну службу Windows.

Звернення до файлових ресурсів по іменах. До файлових ресурсів (протокол SMB) в домені доцільно звертатися через доменне ім'я замість звернення через IP. Крім зручності адміністрування, це дозволяє хосту автентифікуватися за протоколом Kerberos, який є значно більш захищеним, ніж протокол NTLMv2, який задіюється при зверненні по IP до файлового ресурсу. Перехоплення NTLMv2 хешу небезпечне тим, що за допомогою словникової атаки можна відновлювати пароль користувача офлайн, не задіюючи інфраструктуру, що атакується, що не помітно для адміністраторів, на відміну онлайн-атак з перебору паролів. Протокол NTLM, в свою чергу, повинен бути заборонений, бо є більш вразливим. Якщо в системі дозволені обидва протоколи NTLM, можлива ситуація, коли атакуючий може знизити перевагу з NTLMv2 до NTLM, і хост-жертва вибере саму слабку автентифікацію.

Використання демілітаризованої зони. Надійна демілітаризована зона (DMZ) повинна бути налаштована таким чином, щоб уникнути «прокидання» портів з Інтернет в основну мережу. При використанні «прокидання» портів, крім ризику зламу сервісу, існує неявний ризик збору інформації про внутрішню мережу. Ресурси в демілітаризованій зоні повинні бути з двох сторін закриті файерволами (як від внутрішньої мережі, так і від Інтернет), а трафік має бути дозволений тільки мінімально необхідний. З точки зору безпеки системи корисно міркувати, що хост з DMZ вже зламаний, і оцінювати ризики виходячи з цього. Найчастіше в DMZ опиняються нестандартні програми, які несуть специфічну бізнес-логіку, розробляються на замовлення і посередньо перевіряються, наприклад, на WEB вразливості. Штатний фахівець з інформаційної безпеки найчастіше в змозі створити DMZ, але не в змозі перевірити додатки на вразливості. Виходячи з цього припущення і необхідно налаштовувати демілітаризовану зону.

Варіант правильно організованої DMZ зображений на рис. 1.

Сегментація мережі. Доцільно максимально ділити мережі на віртуальні локальні комп'ютерні мережі (VLAN), а також максимально обмежувати широкомовний трафік. Це корисно як з точки зору зручності адміністрування, так і з точки зору безпеки. Сегментація мережі знизить можливості підробки адресу, спростить налаштування мережевого доступу, знизить ймовірність атак за рахунок широкомовних запитів, і, отже, підвищить стабільність роботи.

Повністю ізольований гостьовий WiFi. Гостьовий WiFi повинен бути максимально ізольований від основної мережі (необхідне використання окремої VLAN, окремого проводу від інтернет-маршрутизатора до точки доступу, тощо). Для підвищення безпеки доцільно створити легкий внутрішній DNS сервер спеціально для WiFi, або використовувати публічні DNS в Інтернет.

Також хорошим рішенням буде відключення гостьового WiFi в неробочий час за розкладом на обладнанні.

Віддалений доступ. У корпоративних мережах користувачам повинно бути представлено зручне рішення, що забезпечує індивідуальний захищений віддалений доступ до віртуальних робочих столів, сервісів або додатків.

Пристрої кінцевих користувачів можна захистити за допомогою програмного клієнта. На кожне кінцеве обладнання користувача, що працює за межами контрольованої зони, встановлюється програмний VPN-клієнт, що забезпечує криптографічний захист переданого трафіку і пакетну фільтрацію. Перед тим, як користувачу надається доступ до сервісів компанії, він проходить процедуру автентифікації шляхом введення пароля і цифрового сертифіката відкритого ключа, закритий ключ якого може зберігатися на токені.

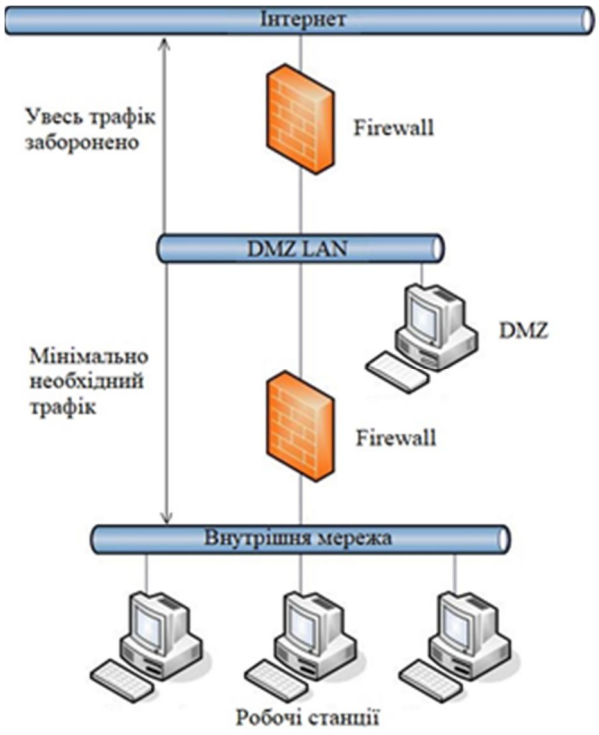

Рис.1. Організація демілітаризованої зони

Можливий варіант захисту пристроїв кінцевих користувачів за допомогою завантажувального носія. Користувачеві надається захищений завантажувальний USB-носій. З нього завантажується замкнена програмна середа, ізольована від операційної системи робочого місця. Ані користувач, ані зловмисник не можуть змінювати або додавати файли у ізольоване середовище, тому немає необхідності в антивірусній програмі і т. п. Автентифікація користувача відбувається за допомогою введення PIN-коду і цифрового сертифіката відкритого ключа, закритий ключ якого зберігється на носії. Дані попередніх сеансів користувача не зберігаються на пристрої.

Шифрування трафіку за допомогою SSL. При роботі по захищеному з'єднанню (найбільш простий приклад — HTTPS) увесь трафік між взаємодіючими точками в мережі шифрується на стороні відправника та дешифрується на стороні одержувача. Для того, щоб його зашифрувати і розшифрувати потрібна пара ключів (асиметричне шифрування). Публічний ключ служить для зашифровки і передається одержувачу даних, а приватний — для дешифрування, він залишається у відправника. Таким чином вузли, між якими встановлюється SSL-з'єднання, обмінюються публічними ключами. Далі, для підвищення продуктивності формується єдиний ключ, який пересилається вже в зашифрованому вигляді і використовується як для шифрування, так і для дешифрування на обох сторонах (симетричне шифрування). Хорошим рішенням вважається захищати шифруванням всі сервіси, де можна застосувати SSL/TLS.

Також необхідно враховувати, що шифрування захищає не тільки від крадіжки облікових даних, але і від підміни трафіку.

Висновки та напрямок подальших досліджень. Розглянуті в роботі варіанти підвищення безпеки передачі і зберігання даних в корпоративних мережах дозволяють підвищити їх захищеність та здатність мережі відбивати атаки зловмисників. Подальші дослідження будуть спрямовані на пошук нових ефективних методів захисту корпоративних мереж та вдосконалення існуючих.

Список літератури

1. **Kurose, James F.** Computer networking: a top-down approach / **James F. Kurose, Keith W. Ross.** - 6th ed., - 2016. - p. 862

2. **Eric Maiwald**. Network Security, - McGraw-Hill Education; 3 edition. - 2012. - p.336

3. **М. М. Браіловський, Т. В. Погребна, О. В. Пташок** Мережі VPN та проблеми їх захисту // Телекомунікаційні та інформаційні технології. - 2014. - № 1. - С.76-80. - Режим доступу: http://nbuv.gov.ua/UJRN/vduikt_2014_1_13

4. **Маркелов К. С., Нейман А. Б.** Безопасность беспроводных сетей // Молодой ученый. — 2012. — №4. — С.63-66. — URL https://moluch.ru/archive/39/4589/

5. **Широчин В. П., Мухин В. Е., Кулик А. В.** Вопросы проектирования средств защиты информации в компьютерных системах и сетях. Киев; «ВЕК+». 2000. — 111 с.

6. **Иванов К. К., Юрченко Р. Н., Ярмонов А. С.** Угрозы безопасности информации в автоматизированных системах // Молодой ученый. — 2016. — №29. — С. 20-22. — URL https://moluch.ru/archive/133/37181/

7. **Мухамадиева З. Б.** Защита информации в информационных системах // Молодой ученый. — 2018. — №9. — С. 34-36. — URL https://moluch.ru/archive/195/48443/

8. **Бирюков А.А.** Информационная безопасность: защита и нападение, - ДМК Пресс, 2016. – 536 с.

9. **Грибунин В. Г.** Комплексная система защиты информации на предприятии. — М.: Академия, 2009. — 415 с

10. **Трунова А. А.** Анализ каналов утечки конфиденциальной информации в информационных системах предприятий // Молодой ученый. — 2016. — №3. — С. 69-72. — URL https://moluch.ru/archive/107/25842/

Рукопис подано до редакції 11.04.2018