– Загалом, категорично не рекомендується використовувати один і той же пристрій чи обліковий запис як для роботи, так і для особистих потреб.

– Тим більше, коли особисті потреби передбачають використання особистої електронною пошти, телефону, планшету чи комп'ютера також і дітьми, чи іншими особами. Якщо щось є робочим інструментом, воно має бути лише для роботи.

– Варто мінімізувати роботу з чутливою інформацію, або знайти спосіб убезпечити її (наприклад – додатковими паролями, засобами шифрування тощо). [3]

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Це – лише базові кроки для "кібергігієни". Є чимало інших хороших практик, якими слід постійно цікавитися. Насамкінець, якщо підозрюєте, що стали жертвою хакерської атаки, чи відбулася іншого роду втрата інформації, про це слід відразу повідомити роботодавця. Поза цим, не слід забувати і про обережність та дотримання законності під час обробки персональних даних інших осіб.

Протидія кіберзлочинності та рівень кібербезпеки на сьогодні є одним із пріоритетних напрямків в політиці країни. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти.

ПОСИЛАННЯ

[1] Holub A. Kiberzlochynnist u vsikh yii proiavakh: vydy, naslidky ta sposoby borotby [Elektronnyi resurs] / A. Holub // Kiberzlochynnist u vsikh yii proiavakh: vydy, naslidky ta sposoby borotby. – 2019. – Rezhym dostupu: https://www.gurt.org.ua/articles/34602/

[2] Hnatiuk S. L. Kiberbezpeka v umovakh rozghortannia chetvertoi promyslovoi revoliutsii (industry 4.0): vyklyky ta mozhlyvosti dlia Ukrainy [Elektronnyi resurs] / S. L. Hnatiuk // Kiberbezpeka v umovakh rozghortannia chetvertoi promyslovoi revoliutsii (industry 4.0): vyklyky ta mozhlyvosti dlia Ukrainy. – 2019. – Rezhym dostupu: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi

[3] Yakubuv A. Robota v smartfoni: domashni zakhody kiberbezpeky pid chas karantynu [Elektronnyi resurs] / A. Yakubov // Robota v smartfoni: domashni zakhody kiberbezpeky pid chas karantynu. – 2020. – Rezhym dostupu: https://www.epravda.com.ua/columns/2020/03/18/658214/

Олександра Дулова
викладач фахових дисциплін,
Відокремлений підрозділ НУБіП України «Ірпінський економічний коледж»,
м. Ірпінь
alexandra_dulova@ukr.net

СИСТЕМИ ЗАХИЩЕНОЇ ПЕРЕДАЧІ ДАНИХ В КОМП'ЮТЕРНИХ МЕРЕЖАХ. СИСТЕМИ ЗАХИСТУ CISCO

Анотація: розглядається питання захисту інформації в комп'ютерних мережах; дослідження засобів захисту даних та інформації в мережі.

Ключові слова: захист, мережа, системи, технології, витоки інформації, cisco

Судячи зі зростаючої кількості публікацій і компаній, що професійно займаються захистом інформації в комп'ютерних системах, рішенню цієї задачі надається велике значення. Однієї з найбільш очевидних причин порушення системи захисту є навмисний несанкціонований доступ (НСД) до конфіденційної інформації з боку нелегальних користувачів. Захист інформації – це комплекс заходів, проведених з метою запобігання

витоку, розкрадання, утрати, несанкціонованого знищення, несанкціонованого копіювання, блокування інформації. Оскільки втрата інформації може відбуватися по технічних, об'єктивних і ненавмисних причинах, під це визначення підпадають також і заходи, пов’язані з підвищенням надійності сервера через відмову або збої в роботі вінчестерів, недоліків у використовуваному програмному забезпеченні.

Перехід від роботи на персональних комп'ютерах до роботи в мережі ускладнює захист інформації з наступних причин:

- велика кількість користувачів у мережі і їх змінний склад. Захист на рівні імені та пароля користувача недостатній для запобігання входу в мережу сторонніх осіб;

- значна довжина мережі і наявність багатьох потенційних каналів проникнення в мережу.

Будь-які додаткові з'єднання з іншими сегментами або підключення до всесвітньої мережі «Інтернет» породжують нові проблеми. Атаки на локальну мережу через підключення до «Інтернету» для того, щоб одержати доступ до конфіденційної інформації, останнім часом отримали широке поширення, що пов’язано з недоліками убудованої системи захисту інформації в протоколах TCP/IP.

Захист інформації в мережі може бути поліпшений за рахунок використання спеціальних генераторів шуму, що маскують побічні електромагнітні випромінювання і наведення, шумо-подавляючих мережних фільтрів, пристроїв зашумлення мережі живлення, скремблерів (шифраторів телефонних переговорів), подавлювачів роботи стільникових телефонів і т.д. Кардинальним рішенням є перехід до з'єднань на основі оптоволокна, вільним від впливу електромагнітних полів, що дозволяють знайти факт несанкціонованого підключення [3].

У цілому засобу забезпечення захисту інформації щодо запобігання навмисних дій у залежності від способу реалізації можна розділити на групи:

- технічні (апаратні) засоби. Це різні по типу пристрої, що апаратними засобами вирішують задачі захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення усе-таки відбулося, доступу до інформації, у тому числі за допомогою її маскування. Першу частину задачі вирішують замки, ґрати на вікнах, захисна сигналізація й ін. Другу – згадувані вище генератори шуму, мережні фільтри, скануючі радіоприймачі і безліч інших пристроїв, що перешкоджають, витоку інформації або дозволяють їх знайти. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

- програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів. Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки – обмежена функціональність мережі, використання частини ресурсів файлу-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їхніх апаратних засобів).

- змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

- організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї й ін.) і організаційно-правових (національні законодавства і правила роботи, установлювані керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки – висока залежність від

суб'єктивних факторів, у тому числі від загальної організації роботи в конкретному підрозділі.

В силу того, що за різними оцінками від 80 до 95 відсотків вірусів проникає в корпоративні мережі через електронну пошту, перевірка поштового трафіку є одним з найважливіших завдань забезпечення антивірусної безпеки організації. При цьому під поштовим трафіком розуміється SMTP-потік. Антивірусні комплекси для захисту поштових систем не перевіряють дані, що передані по протоколах IMAP й POP при обігу користувачів, їх персональної організації ящика, оскільки це - завдання антивірусного комплексу для захисту робочих станцій. Завданням антивірусного комплексу для поштової системи є перевірка й усього потоку листів, що надходять і виходять із поштової системи організації.

Використання антивірусних комплексів для поштових систем необхідно для забезпечення безпеки інформації, однак виникає питання які комплекси і як повинні бути використані для захисту мереж.

Вибір засобів захисту поштової системи опирається на з'ясування двох ключових факторів:

• схема побудови поштової системи організації;

• визначення схеми роботи антивірусного комплексу.

Більшість погроз, і це не дивно, орієнтовано на ОС сімейства Windows. Під керуванням ОС цього сімейства функціонує левина частка всіх комп'ютерів у світі, що створює великий простір для діяльності авторів вірусів, на що б ця діяльність не була спрямована - задоволення особистих амбіцій, придбання популярності, одержання прибутку або всього разом [1].

Для зараження комп'ютера під керуванням Microsoft Windows застосовуються практично всі способи проникнення й активізації. Використаються всілякі канали проникнення, уразливості в системних і прикладних програмах, методи соціальної інженерії. Відповідно, ПО для захисту робочих станцій Windows повинне мати засоби для протидії по можливості всім видам погроз.

Розкрадання інформації звичайно відбувається непомітно для персоналу служби інформаційної безпеки або мережі. Отже, необхідно забезпечити можливість швидкої і автоматичної реакції системи безпеки на підозрілу мережну активність. Стратегія мережі самозахисту, дозволяє створити комплексну систему захисту від розкрадання інформації.. Тільки Cisco пропонує системний підхід до захисту, що не має аналогів, бізнес процесів на основі розумного об'єднання мережних рішень, технологій захисту і служб безпеки. Самозахищаюча мережа складається з трьох компонентів (систем), кожний з яких виконує конкретні функції. Ці системи працюють спільно для виявлення і блокування спроб розкрадання корпоративної інформації.

Забезпечення конфіденційності інформації є важливою задачею для будь-якої організації. Користувачі вимагають забезпечення конфіденційності при передачі даних і голосу по каналах зв'язку, а також вживання заходів по запобіганню несанкціонованого доступу до персональної інформації. Технологія віртуальних приватних мереж (VPN) дозволяє системі безпечних з'єднань Cisco пригнічувати спроби розкрадання даних, відео і голосу в IP-мережах, забезпечуючи цілісність і конфіденційність інформації, переданої через загальнодоступні і приватні мережі.

Мережі повинні мати нагоду протистояти як зовнішнім, так і внутрішнім атакам. З метою запобігання розкрадання інформації система захисту від загроз Cisco забезпечує захист від зловмисної активності, націленої на кінцеві вузли, такі як настільні комп'ютери і сервери, і, використовуючи логічний механізм, виконує виявлення, розпізнавання і блокування підозрілої поведінки в будь-якій крапці мережі.

Перша лінія захисту мережі організації - визначити користувачів і пристрої, які мають доступ до мережі, перевірити стан таких пристроїв і уточнити має рацію і привілеї, що дозволяють цим пристроям отримати доступ до ресурсів. Система довір'я і ідентифікації Cisco перешкоджає розкраданню інформації, надаючи доступ до корпоративної мережі тільки довіреним користувачам і пристроям, причому ці користувачі і пристрої не можуть отримати доступ до заборонених для них інформаційних ресурсів [2].

Перший крок до організації захищеного мережного середовища – це перевірка ідентичності і повноважень доступу користувачів. Система довір'я і ідентифікації Cisco забезпечує ідентифікацію користувачів за допомогою стандартних протоколів і технологій аутентифікації, таких як протокол 802.1X і технологія аутентифікації, авторизації і обліку (AAA), інтегрованого в комутатори Cisco Catalyst® і маршрутизатори Cisco. Після перевірки ідентичності користувача йому можна надати привілеї доступу. Сервер Cisco ACS (Cisco Secure Access Control Server) управляє настройкою політик і доступом в мережу. Сервер Cisco ACS дозволяє адміністраторам контролювати доступ користувачів до різних сегментів мережі, дозволяти використовування різних мережних служб окремим користувачам або групам користувачів і реєструвати всі дії користувачів в журналі.

Перед тим, як дозволити пристрою доступ в мережу, його необхідно перевірити на відповідність політиці безпеки для кінцевих вузлів. Система контролю доступу Cisco NAC (Cisco Network Admission Control) зіставляє дані про стан системи пристрою з діючою політикою безпеки. Взаємодіючи з галузевими партнерами, такими як Trend Micro і IBM, мережа, використовуючи інтелектуальні механізми Cisco NAC, визначає ступінь відповідності кінцевого вузла діючим політикам безпеки і на підставі отриманої інформації дозволяє або забороняє доступ.

ПОСИЛАННЯ

1.Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windiws Sockets. - Диалог - МИФИ, 1996.

2. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994.

3. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994.

УДК 004.738

V. Lakhno [1][0000-0001-9695-4543],
[1] Professor, National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
A. Blozva [2][0000-0002-4377-0916]
[2] National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
G. Zhilkishbayeva [3][0000-0001-9955-5994],
[3] Yessenov University, Aktau, Kazakhstan,
A. Asselkhan [4][0000-0001-7233-4104]
[4] Abai Kazakh National Pedagogical University, Almaty, Kazakhstan,

ЗАСТОСУВАННЯ ПІДХОДІВ ЗОНАЛЬНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗВО

Анотація У даній публікації розглянуто проблеми побудови компютерних мереж ЗВО, які загрози виникають та можливість забезпечити комплексну безпеку всіх користувачів.