УДК 004.056:061.68 DOI: 10.31673/2518-7678.2020.011014

Черноштан А.М., Власов О.М., д.т.н.

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ ПРИ ВІДДАЛЕНОМУ УПРАВЛІННІ

Chernoshtan A.M., Vlasov O.M. Technique for Securing Corporate Network Communication in Remote Management. This article describes how to secure your corporate communications network with remote management. The principles of corporate network security enhancement are presented taking into account the developed methodology. The review of modern technologies of protection of corporate networks and methods of influence of malefactors on them is made. The obtained results are analyzed and systematized. The feasibility of performing each of the considered methods of protection under specific conditions is investigated.

Keywords: corporate network, technical protection of information, automated systems, intrusion detection systems.

Черноштан А.М., Власов О.М. Методика забезпечення захисту корпоративної мережі зв'язку при віддаленому управлінні. У статті розглянуто методику забезпечення захисту корпоративної мережі зв'язку при віддаленому управлінні. Показано принципи підвищення безпеки корпоративних мереж з урахуванням розробленої методики. Виконано огляд сучасних технологій захисту корпоративних мереж та методів впливу зловмисників на них. Проаналізовано та систематизовано одержані результати. Досліджено доцільність виконання кожного із розглянутих методів захисту за конкретних умов.

Ключові слова: корпоративна мережа, технічний захист інформації, автоматизовані системи, системи виявлення вторгнень.

Черноштан А.М., Власов О.М. Методика обеспечения защиты корпоративной сети связи при удаленном управлении. В статье рассмотрена методика обеспечения защиты корпоративной сети связи при удаленном управлении. Показано принципы повышения безопасности корпоративных сетей с учетом разработанной методики. Выполнен обзор современных технологий защиты корпоративных сетей и методов воздействия злоумышленников на них. Проанализированы и систематизированы полученные результаты. Исследована целесообразность выполнения каждого из рассмотренных методов защиты в конкретных условиях.

Ключевые слова: корпоративная сеть, техническая защита информации, автоматизированные системы, системы обнаружения вторжений.

Вступ

В наш час велику популярність набули глобальні мережі особливо Internet. І в зв'язку з цим виникли проблеми з захистом інформації. Питання захисту інформації стало невід'ємною частиною любої системи яка працює з комерційно значущою інформацією. При використанні Internet в комерційних межах а також для з'єднання частин компаній і організацій виникають проблеми захищеності інформації яка проходить через мережу і обмеження доступу зовнішніх користувачів до внутрішніх мереж. Захист інформації стоїть на першому місці по актуальності і поставлених задач.

Актуальністю захисту інформації в корпоративних мережах є запобігання викрадення інформації. Все більше і більше людей отримують доступ до мережі Internet, а хакерів і "script kiddes" на сьогоднішній день більше ніж колись. Питання захисту корпоративної мережі не варто відкладати на майбутнє адже це може обернутись трагедією для компанії.

Виклад основного матеріалу дослідження

Говорити про те, що інформаційна безпека стала частиною корпоративних мереж в нашій країні можна з великим сумнівом. Необхідність забезпечувати надійну безпеку інформації освідомили тільки великі компанії, але й вони до недавнього часу сприймали проблеми тільки з технічної сторони, яка була поставлена тільки з сторони встановлення програмного забезпечення для захисту інформації такого як антивірусного програмного забезпечення, міжмережевих екранів, програм для моніторингу мереж і виявлення вторгнень, несанкціонованого доступу і віртуальних частин мереж. За рекомендаціями дослідницьких фірм, основним напрямком забезпечення безпеки слід спрямувати на розробку політики безпеки і супутніх їй документів. Політика безпеки є найдешевшим і одночасно найефективнішим засобом забезпечення інформаційної безпеки. Крім того, якщо політика сформульована, то вона є і керівництвом щодо розвитку і вдосконалення системи захисту. Корпоративна мережа - взаємопов'язана сукупність мереж, служб передачі даних і Телеслужби, призначена для надання єдиного захищеного мережевого простору обмеженому рамками корпорації колу користувачів.

Для існуючих корпоративних автоматизованих систем властиво:

1. Використання корпораціями розподіленої моделі обчислень. Однак в останні 5-10 років у нашій країні і за кордоном набирають популярність технології тонкого клієнта.

2. Невіддільність корпоративних додатків від функціональних підрозділів корпорації, оскільки частина прикладного коду розташовується на станції-клієнті.

3. Необхідність одночасного контролю декількох локальних обчислювальних мереж, необхідність обміну центральній консолі повідомленнями з платформами адміністрування.

4. Широкий спектр використовуваних способів подання, зберігання і передачі інформації.

5. Інтеграція даних різного призначення, що належать різним суб'єктам, в рамках єдиних баз даних. І розміщення необхідних деяким суб'єктам даних у віддалених вузлах мережі (приклад, текстові звіти, збережені на робочих станціях).

6. Абстрагування власників даних від фізичних структур і місця розміщення даних.

7. Участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій. Безпосередній і одночасний доступ до ресурсів (у тому числі і інформаційним) великої кількості користувачів (суб'єктів доступу) різних категорій.

8. Високий ступінь різнорідності засобів обчислювальної техніки і зв'язку, а також програмного забезпечення.

9. Відсутність спеціальної програмно-апаратної підтримки засобів захисту у функціональних технічних засобах, які у системі.

При створенні інформаційної інфраструктури корпоративної автоматизованої системи (АС) на базі сучасних комп'ютерних мереж неминуче виникає питання про захищеність цієї інфраструктури від загроз безпеки інформації. А саме: наскільки адекватні реалізовані в АС механізми безпеки існуючим ризикам; чи можна довіряти цій АС обробку (зберігання, передачу) конфіденційної інформації; чи є в поточній конфігурації АС помилки, що дозволяють потенційним зловмисникам обійти механізми контролю доступу; чи містить встановлене в АС програмне забезпечення (ПЗ) уразливості, які можуть бути використані для злому захисту; як оцінити рівень захищеності АС і як визначити чи є він достатнім в даному середовищі функціонування; які контрзаходи дозволять реально підвищити рівень захищеності АС; на які критерії оцінки захищеності слід орієнтуватися і які показники захищеності використовувати. Такими питаннями рано чи пізно задаються всі фахівці IT-відділів, відділів захисту інформації та інших підрозділів, відповідають за експлуатацію та супровід АС. Відповіді на ці питання далеко неочевидні. Аналіз захищеності АС від загроз безпеки інформації є не простою задачею. Уміння оцінювати і управляти ризиками, знання

типових загроз і вразливостей, критеріїв і підходів до аналізу захищеності, володіння методами аналізу та спеціалізувати інструментарієм, знання різних програмно-апаратних платформ, що використовуються в сучасних комп'ютерних мережах - ось далеко не повний перелік професійних якостей, якими повинні володіти фахівці, провідні роботи з аналізу захищеності АС. Аналіз захищеності є основним елементом таких взаємно пересічних видів робіт як атестація, аудит та обстеження безпеки АС [4].

На практиці завжди існує велика кількість непіддатних точній оцінці можливих шляхів здійснення загроз безпеки в відносно ресурсів АС. В ідеалі кожен шлях здійснення загрози повинен бути перекритий відповідним механізмом захисту. Дане умова є першим фактором, що визначає захищеність АС. Другим чинником є міцність існуючих механізмів захисту, що характеризується ступенем опірності цих механізмів спробам їх обходу або подолання. Третім фактором є величина збитку, що наноситься власникові АС у разі успішного здійснення загроз безпеки [1].

На практиці отримання точних значень наведених характеристик утруднено, так як поняття загрози, збитку і опірності механізму захисту тяжко формулюючи. Наприклад, оцінку збитку в результаті несанкціонованого доступу до інформації політичного та військового характеру точно визначити взагалі неможливо, а визначення вірогідності здійснення загрози не може базуватися на статистичному аналізі. Оцінка ступеня опірності механізмів захисту завжди є суб'єктивною.

Розгляд можливих дій зловмисників необхідно вести в умовах, які існують в сучасних вітчизняних компаніях. Розглянемо типову корпоративну мережу, побудовану на апаратних і програмних засобах, які широко використовуються в корпоративних мережах приватних і державних організацій.

Апаратні засоби корпоративних мереж включають фізичну середовище і обладнання передачі даних. Внаслідок обмеженого застосування в даний час бездротових мереж, типова корпоративна мережа побудована на основі кабельної системи, що представляє собою виту пару 5-ї категорії. Сучасні корпоративні мережі розробляються з застосуванням комутаторів (switch) і концентраторів (hub). Обидва цих мережевих пристрої служать для об'єднання комп'ютерів в локальні мережі. Хоча концентратори в даний час витісняються комутаторами, тим не менш, у багатьох мережах організацій концентратори широко використовуються в силу своєї дешевизни. Комутатор представляє собою більш складне мережеве пристрій. І як наслідок розрізняються за набору підтримуваних функцій. Найбільш складні (і дорогі) моделі називаються керованими інтелектуальними комутаторами і володіють власним IP-адресою, підтримкою віддаленого адміністрування, засобами організації віртуальних мереж (VLAN) і розвиненим набором засобів захисту. Вартість інтелектуальних комутаторів може досягати 2000 доларів, що ускладнює їх купівлю невеликими організаціям. програмні засоби, що використовуються у типовій мережі, також є стандартними для більшості організацій. Робочі станції на базі операційних систем (ОС) Windows 95, 98, NT4 Workstation, 2000, XP (за статистикою в 90 % всіх організацій у світі використовуються робочі станції на базі Windows різних версій). Сервера на базі ОС Windows NT4 Server/Terminal Server Edition, 2000 Server, 2003 Server. Пакети популярного програмного забезпечення (ПО) для офісної роботи: 1С, MS Outlook, MS Office 97/2000/XP Серверне ПЗ: 1С, MS SQL Server, MS Exchange [5].

В якості засобів захисту використовуються міжмережеві екрани: Agnitum Outpost Firewall, Kerio Personal Firewall, Kaspersky Anti-Hacker, Norton Personal Firewall; системи виявлення атак Black ICE, Snort, RealSecure.

Створення політики безпеки організації та контроль її виконання. Політика має включати:

- Стратегію захисту IT-інфраструктури організації.

• Набір правил, за якими створюється, обробляється та зберігається інформація на підприємстві.

• Правила своєчасного оновлення ПЗ та відповідальність працівників.

• Резервне копіювання та відновлення даних.

• План дій з локалізації, блокування розповсюдження, та відновлення після атак.

Запровадження правил використання облікових записів в організації, що включають:

o Персоніфікований адміністративний доступ. Заборона використання спільних адміністративних облікових записів.

o Використання різних облікових записів для виконання різних адміністративних задач:

o для адміністрування домену;

o для адміністрування серверів (різні записи для різних функцій);

o для адміністрування ПК користувачів;

o для адміністрування власного ПК.

o Заборона здійснювати регулярні задачі з використання адміністративних облікових записів:

o Адміністратори повинні працювати на своїх ПК під стандартними обліковими записами з правами рівня звичайного користувача.

o Робота з адміністрування інформаційних систем повинна здійснюватися з окремого виділеного термінального сервера управління (або спеціалізованих систем PAM), а не безпосередньо з призначеного для користувача ПК.

o Використання адміністратором для певних робіт відповідного облікового запису має суворо контролюватися.

o Заборона використання облікових записів адміністраторів домену для задач, що не пов’язані з адмініструванням контролерів доменів.

Регулярне навчання всіх користувачів організації є основою інформаційної безпеки та

регулярне навчання і підвищення кваліфікації ІТ-фахівців та адміністраторів, та проведення тестових атак.

Технічними заходи є:

• Впровадження контролю на периметрі корпоративної мережі

• Встановлення та налаштування мережевих екранів з функціями контролю та протидії вторгнень.

• Встановлення та налаштування веб-шлюзу безпеки (для контролю доступу користувачів організації до мережі Інтернет)

• Встановлення та налаштування поштового шлюзу безпеки (для захисту корпоративної пошти від спаму та зовнішніх загроз)

• Безпечне віддалене керування через WAN та Інтернет-канали зв’язку повинне здійснюватися лише за допомогою VPN-технологій з використанням належного рівня шифрування (AES-256 та вище).

• При віддаленому керуванні необхідно обов’язково використовувати термінальний сервер (Jump Host) та моніторинг з фіксацією виконаних дій.

• Контроль локальної мережі

• Налаштування сегментації локальної мережі згідно функціонального призначення (для мережевого відділення особливо критичних систем та сервісів).

• Налаштування технологій ізоляції портів (Port Isolation/Private VLAN) на комутаторах доступу користувачів (для заборони прямої взаємодії між користувацькими системами)

• Налаштування технологій протидії атакам типу ARP Spoofing та фальшивих DHCP-серверів (для унеможливлення перехоплення трафіку)

• Регулярне оновлення системного та прикладного ПЗ (Patch Management).

• Встановлювати актуальне антивірусне програмне забезпечення на серверних та користувацьких системах організації.

• Створити рішення для контролю підключення периферійних пристроїв та зйомних носіїв до робочих станцій організації [3].

Висновки

Для того щоб забезпечити надійний захист корпоративних мереж зв'язку на сьогодні і на найближче майбутнє, у системі інформаційної безпеки повинні бути реалізовані самі прогресивні й перспективні технології інформаційної безпеки. До них відносяться:

- комплексний підхід до формування інформаційної безпеки, що забезпечує раціональне об'єднання технологій і засобів інформаційного захисту;

- застосування захищених віртуальних мереж VPN для захисту інформації, переданої по відкритих каналах зв'язку;

- криптографічне перетворення даних для забезпечення цілісності, дійсності й конфіденційності інформації;

- застосування міжмережевих екранів для захисту корпоративної мережі від зовнішніх погроз при підключенні до загальнодоступних мереж зв'язку;

- керування доступом на рівні користувачів і захист від несанкціонованого доступу до інформації [2].

Список використаної літератури

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем [Электронный ресурс]/ А. Астахов //ISO27000.ru.

2. Искусство управления информационной безопасностью: сайт. – Режим доступа: http://iso27000.ru/chitalnyizai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem (10.01.2020).

3. Крысин В.А. Безопасность предпринимательской деятельности / Крысин В.А. - М: Финансы и статистика, 2010. — 246 с.

4. Концепція захисту IT-інфраструктури від сучасних загроз [Електронный ресурс]. – Режим доступу: URL: https://netwave.ua/kontseptsiya-zahy-stu-infrastruktury-vid-suchasny-h-zagroz/ (10.01.2020).

5. Ситник В.Ф. Системи підтримки прийняття рішень: Навч. посіб. – К.: КНЕУ, 2009. – 614 с.

6. Соколов. А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. – 656 с.

Автори статті

Черноштан Аліна Миколаївна – студентка, Державний університет телекомунікацій, Київ, Україна.

Власов Олександр Миколайович – доктор технічних наук, професор, професор кафедри телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Chernoshtan Alina Mykolaivna – student, State University of Telecommunications, Kyiv, Ukraine.

Vlasov Oleksandr Mykolaiovych – sciences doctor (technic), professor of the Department of Telecommunication Systems and Networks, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 12.01.2020 р. Рецензент: д.т.н., доц. В.Ф. Заїка