Д. С. Трофимов

РАЗРАБОТКА ОТКАЗОУСТОЙЧИВОЙ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

Рассмотрены различные способы защиты информации, позволяющие достичь достаточного уровня защиты корпоративной информации и бесперебойной работы сотрудников организации, разработана корпоративная инфраструктура.

Введение

Любой корпоративной инфраструктуре необходимы самые современные технологии защиты информации и способы достижения бесперебойной работы. Проблемы, возникающие на техническом уровне, возрастают с высокой интенсивностью. Изучение и внедрение новых способов защиты информации позволит предотвратить потерю и шифрование конфиденциальной информации.

I. Межсетевой экран

За защиту информации между внутренней корпоративной и глобальной сетями отвечает межсетевой экран (далее – МЭ), известный как Брандмауэр или Файрвол. МЭ является контрольным пунктом на границе двух сетей. Граница может лежать между внутренней сетью организации и внешней сетью Интернет, а может применяться для разграничения внутренних подсетей корпоративной сети организации. [1] Задачами МЭ являются контроль всего трафика, входящего во внутреннюю корпоративную сеть и трафика, исходящего из внутренней корпоративной сети. МЭ удобно представить в виде системы фильтров. Каждый фильтр на основе анализа проходящих через него данных, принимает решение – пропустить дальше, перебросить за экран, блокировать или преобразовать данные.

II. Система обнаружения атак

Система обнаружения атак способна перехватывать только известные способы атак. Обнаружение неизвестной атаки является трудной задачей. Современные системы обнаружения атак способны контролировать работу сетевых устройств и операционной системы, выявлять несанкционированные действия и автоматически реагировать на них практически в реальном масштабе времени. При анализе текущих событий могут учитываться уже произошедшие, что позволяет идентифицировать атаки, разнесенные во времени, и тем самым прогнозировать будущие события. [2] Типовая структура системы обнаружения вторжений представлена на рисунке 1 и включает в себя следующие компоненты: 1. Сенсоры (средство сбора информации); 2. Анализаторы (средство анализа информации); 3. Хранилище; 4. Рабочее место администратора. Различают сетевые и хвостовые сенсоры. Сетевые сенсоры осуществляют перехват сетевого трафика, хостовые сенсоры используют в качестве источников информации журналы регистрации событий ОС, СУБД и приложений. Анализатор, размещаемый на сервере безопасности, осуществляет централизованный сбор и анализ информации, полученной от сенсоров.

Рис. 1 – Типовая структура системы обнаружения вторжений

III. Вывод

Рассмотренные способы защиты позволяют достичь частичной защиты данных и бесперебойной работы предприятия. Из рассмотренных основных способов защиты: система обнаружения атак, фильтры позволяют минимизировать шанс потери конфиденциальной информации.

1. Основные методы защиты корпоративных сетей связи предприятия: https://studfiles.net/preview/1853728/page:17/
2. Системы обнаружения атак, интернет ресурс: https://www.bytemag.ru/articles/detail.php?ID=6608
3. Шаньгин В.Ф. Информационная безопасность. – Москва: ДМК Пресс, 2014. – 702 с.

Трофимов Дмитрий Сергеевич, магистрант 1 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлекстроники, dmitrii.trofimov1387@gmail.com

Научный руководитель: Павлова Анна Валентиновна, доцент кафедры систем управления Белорусского государственного университета, кандидат технических наук, pavlova@bsuir.by