АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ

Ф.А. Бабенко, Т.П. Тынкович

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был невелик, так как зависимость мировой экономики от информационных технологий была мала. В настоящее время в условиях значительной зависимости бизнеса от электронных средств доступа и обмена информацией и постоянно растущего числа атак ущерб от самых незначительных атак, приводящих к потерям машинного времени, исчисляется миллионами долларов, а совокупный годовой ущерб мировой экономике составляет десятки миллиардов долларов.

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации, сосредоточение в базах данных информации различного уровня важности и конфиденциальности, расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети, увеличение числа удаленных рабочих мест, широкое использование глобальной сети Internet и различных каналов связи, автоматизация обмена информацией между компьютерами пользователей.

Корпоративная информационная система представляет собой сложную структуру, в которой объединены различные сервисы, необходимые для функционирования компании. Эта структура постоянно меняется – появляются новые элементы, изменяется конфигурация существующих. По мере роста системы обеспечение информационной безопасности и защита критически важных для бизнеса ресурсов становятся все более сложной задачей.

Для того чтобы выявить недостатки защиты различных компонентов и определить потенциальные векторы атак на информационные ресурсы, проводится анализ защищенности. Эффективный способ анализа – тестирование на проникновение (пентест), в ходе которого моделируется реальная атака злоумышленников. Цель тестирования – обнаружить возможные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу от обслуживания, а также спрогнозировать возможные финансовые потери и экономические риски.

Технологии информационной безопасности очень быстро устаревают, решение, оптимальное для предприятия заказчика на данный момент, не будет таковым через некоторое время. Поэтому многие специалисты по информационной безопасности рекомендуют проводить penetration test на регулярной основе, наилучшее решение – ежегодно.

Литература

1. Конеев И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с

2. Олифер В.Г. Олифер Н.А. Компьютерные сети: 2-ое изд. – М.: Вильямс, 2007. – 1410 с.

3. Коллинз М. Защита сетей. Подход на основе анализа данных. – М.: ДМК, 2019. – 308 с.