КОНЦЕПЦИЯ АДАПТИВНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Полещук В.С., Ширинский В.П., Некрашевич И.Г.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ширинский В.П. – к.т.н.,доцент

В работе приводится описание модели адаптивной безопасности сети. Дано обоснование подхода к адаптивному управлению безопасностью информационных систем. Приведены основные классификационные признаки объектов управления в концепции адаптивного управления.

Непрерывное развитие сетевых технологий при отсутствии постоянно проводимого анализа их безопасности и нехватки ресурсов для обеспечения защиты приводит к тому, что с течением времени защищенность корпоративных инфологических систем падает, так как появляются новые неучтенные угрозы и уязвимости системы.

Адаптивный подход к безопасности позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Адаптивная безопасность сети состоит их трех основных элементов:

- технологии анализа защищенности;
- технологии обнаружения атак;
- технологии управления рисками.

Анализ защищенности – это поиск уязвимых мест в сети. Сеть состоит из соединений, узлов, рабочих станций, приложений и баз данных. Все они нуждаются как в оценке эффективности их защиты, так и в поиске неизвестных уязвимостей в них. Технология анализа защищенности исследует сеть и ищет слабые места в ней, обобщает эти сведения и печатает по ним отчет.

Если система, реализующая эту технологию, содержит и адаптивный компонент, то устранение найденной уязвимости будет осуществляться не вручную, а автоматически. Технология анализа защищенности является действенным методом, позволяющим реализовывать политику сетевой безопасности прежде, чем будет осуществлена попытка ее нарушения.

Обнаружение атак является процессом оценки подозрительных действий, происходящих в корпоративной сети. Обнаружение атак определяется с помощью анализа журналов регистрации ОС или сетевого трафика.

Адаптивный компонент модели адаптивного управления безопасностью отвечает за модификацию процесса защищенности.

Оценка риска состоит в выявлении и ранжировании уязвимостей (по степени серьезности ущерба потенциальных воздействий), подсистем сети (по степени критичности), угроз (исходя из вероятности их реализации) и т.д.

Поскольку конфигурация сети постоянно меняется, то процесс оценки риска должен производиться постоянно.

Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы и реагировать на них эффективным способом.

Список использованных источников:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.: ил. — (Профессиональное образование)

2. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. - 616 с.

3. Лукацкий А. Обнаружение атак (2-е изд.) . Серия "Мастер систем". - СПб.: БХВ-Петербург, 2003. - 608 с.: ил.