СЕКЦИЯ 1. ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИКА АУДИТА УЯЗВИМОСТЕЙ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

А.А. Зубко, А.М. Прудник

С ростом числа пользователей банковского дистанционного обслуживания, растет и количество угроз для этих систем. Злоумышленники могут использовать уязвимости не только клиента банка, но и самого банка, а вернее системы ДБО. Используя эти уязвимости, злоумышленник может получить большие возможности по манипуляции данными в системе ДБО, в том числе может управлять счетами клиентов. Поэтому есть необходимость в проведении аудита уязвимостей системы ДБО по определенному методу.

Этап 1. Выявление уязвимостей, который начинается с создания и поддержания текущей базы данных всех IP-устройств, подключенных к сети. Организации должны категоризировать устройства согласно их ценности для бизнеса, чтобы расположить их по приоритетам для будущего процесса устранения уязвимостей. Элементы в базе данных включают все аппаратные средства, программное обеспечение, приложения, сервисы и конфигурации. Необходимо очень ответственно подойти к данному этапу. Правильно организованный контроль за этой работой даст компании два преимущества: будет идентифицировано, какие уязвимости влияют на определенные параметры IT инфраструктуры и бизнес процессы, кроме того, точная инвентаризация гарантирует, что в процессе исправления будут отобраны и применены правильные патчи. Проведение инвентаризации также помогает ускорить процесс сканирования, поскольку сокращается время на поиск устройств с одного рода уязвимостями.

Этап 2. Поиск уязвимостей путем сканирования всей инфраструктуры на наличие слабых мест. Система сканирования периодически тестирует и анализирует IP-устройства, сервисы и приложения. Отчет после сканирования указывает на фактические слабые места и на то, что именно нужно исправить.

Этап 3. Распределить уязвимости по категориям. Корпорация Microsoft, например, выделяет четыре категории устранения риска: критически важный, важный, умеренный и низкий с соответствующими показателями.

Этап 4. Процесс исправления уязвимостей. Вносятся изменения в IT-инфраструктуру, применяются различные патчи. Иногда высокая стоимость внесения исправлений вместе с большим объемом недостатков в приложениях от поставщиков вынуждают организации откладывать процесс устранения недостатков на неопределенное время. К сожалению, задержка может оказаться фатальной, поскольку потенциальные слабые места быстро обнаруживаются злоумышленниками — как показывают исследования, временной интервал между появлением угрозы и вторжением постоянно сокращается. Поэтому важно устранить уязвимость как можно быстрее и тем самым минимизировать риски.

Литература

1. *Лямин Л.* Системы Применение технологий электронного банкинга: риск-ориентированный подход. М., 2011.

2. https://www.qualys.com/forms/cloud-agent/

МЕТОДИКА ОБОСНОВАНИЯ КОЛИЧЕСТВА ПОДРАЗДЕЛЕНИЙ КОМПЛЕКСНОГО ТЕХНИЧЕСКОГО КОНТРОЛЯ

В.Н. Корделюк

Армии иностранных государств проводят по отношению к другим мероприятия по добыванию, обработке и анализу разведывательной информации в интересах обеспечения преимуществ своему государству в военной сфере. В связи с этим в целях защиты информации о своих объектах необходимо проводить различные мероприятия противодействия разведкам, в том числе и их техническим средствам.

Обязательными составляющими мероприятий противодействия техническим средствам разведки (ПД ТСР) являются мероприятия комплексного технического контроля (КТК) [1], основными задачами которого являются выявление и анализ демаскирующих признаков своих