«ЗАКАТ СИСТЕМНЫХ СРЗИ»

1. Системные или прикладные средства защиты

Прежде всего, необходимо определиться, что мы понимаем под «системными» средствами защиты информации (СрЗИ). По сути, системные СрЗИ обеспечивают защиту информации на уровне операционной системы и оперируют объектами системного уровня.

К объектам системного уровня относятся: файлы, каталоги, порты ввода-вывода, устройства, носители и т.п. К системным СрЗИ можно отнести такие средства защиты как: «SecretNet», «Страж NT», «Соболь».

Развитие IT в итоге привело к появлению прикладных объектов доступа и соответственно прикладного уровня защиты как самостоятельного направления.

Чтобы понять разницу между системным и прикладным уровнями защиты информационной системы рассмотрим следующий пример.

На сервер установлена ОС Windows и СУБД в которой обрабатывается конфиденциальная информация несколькими пользователями. Системные средства защиты ОС Windows осуществляют защиту информации на уровне ОС и файлов СУБД. Встроенные в СУБД механизмы осуществляют защиту на уровне прикладных объектов СУБД (поля, записи, функции и т.п.).

В связи с бурным развитием информационных систем, типы прикладных объектов весьма многообразны и часто специфичны для конкретных версий прикладных систем. К прикладным объектам могут относиться: документы, сессии, функции и т.п. Многообразие прикладных систем – основная причина, по которой системные СрЗИ уходят на второй план.

Итак, СрЗИ можно классифицировать по типам объектов доступа на системные и прикладные. При этом важно понимать, что прикладные СрЗИ, как правило, встроены в прикладные системы еще на этапе их разработки.

2. Причины

Первая причина, по которой мы можем говорить о закате системных СрЗИ, это миграция информационных систем на прикладной уровень. Если 20 лет назад пользователи в основном работали с файлами, то современные информационные системы представляют данные на других уровнях абстракции.

Вторая причина заключается в многообразии и, часто, уникальности прикладных систем. Разработчики СрЗИ не в состоянии охватить и контролировать информационные потоки прикладного уровня.

3. Соответствие СрЗИ прикладных систем, требованиям регуляторов

В редких случаях разработчики прикладных систем учитывают требования национальных регуляторов (не своих) при включении механизмов защиты в архитектуру своих продуктов. Для этого существует масса причин, прежде всего экономического характера. Продукт должен продаваться! Все остальное вторично. Например, если Продукт готовится к массовой продаже и рынок готов его потребить, но условием является ограничение - выполнение требований регулятора, то очевидно, ожидая большие продажи, разработчик приложит силы для внедрения в продукт всех механизмов защиты, даже тех, которые он может посчитать вздорными "хотелками" регулятора. Если же рынок не интересен или требования слишком "странные" разработчик включает режим "у нас прекрасные продукты, как их будут "легализовывать" заинтересованные потребители - их проблемы". В этом случае разработчики целевых систем вынуждены или пытаться адаптировать продукты или подстраивать целевую систему под ограничения продукта.

4. Где же взять специалиста по прикладным СрЗИ?

Разнообразие прикладных систем сводит на нет наличие универсальных специалистов и универсального их обучения. Раньше, в эпоху рассвета системных СрЗИ почти все СЗИ компании мог сопровождать один универсальный специалист. Сегодня это уже не так. Часто специалист, обслуживающий прикладную систему лучше понимает не только функциональные подсистемы, но и работу механизмов защиты.

4.1. Как в этом случае обновлять ИБ компетенции?

Только через специализированные курсы или внутренние семинары в компании, по прикладным системам, которые входят в состав используемых ИС!

При всем многообразии прикладных систем среди них есть лидеры. Учебные центры чтобы как-то расширить число обучаемых уже рассматривают вопрос о создании обучающих кейсов по продуктам ORACLE, HP, CISCO, MICROSOFT, SAP, IBM, INTEL, и т.д. Альтернативой можно считать курсы и экзамены,

организованные самими вендорами. При этом, отправить на курс по ИБ лучше специалиста по используемому SAP, а не специалиста по системным СрЗИ.

4.2. Новый облик службы ИБ

Все это влияет и формирует новый облик службы ИБ. В эпоху прикладных систем эффективнее "подтянуть" ИТ специалиста в направлении ИБ по прикладной системе чтобы он в повседневной деятельности использовал знания, чем нанимать универсального специалиста по ИБ и обучать его в плане функционирования прикладных систем, при том, что постоянная необходимость в таком специалисте ставится под вопрос.

Новый облик службы ИБ может включать:

- Специалиста по политикам ИБ;
- Юриста;
- Специалиста по системным СрЗИ;
- Специалистов по используемым прикладным информационным системам «подтянутые» по теме ИБ и механизмов защиты соответствующих продуктов (необходимое количество).

5. Выводы

Мы вступили в эпоху прикладных информационных систем и средств защиты информации.

Системные средства защиты отошли на второй план. Основная активность наблюдается в сегменте прикладных средств защиты.

ИТ специалисты, формирующие и обслуживающие прикладные информационные системы вынуждены заниматься и вопросами ИБ в виду того, что они лучше понимают механизмы защиты их роль и особенности в прикладных информационных системах.