ВирусБлокАда

Корпоративные предложения для банковского сектора.

Защита информации от несанкционированного доступа

Дмитрий Ледяев, специалист по информационным технологиям компании «ВирусБлокАда».

Внешние электронные носители (в первую очередь USB-накопители) относительно дешевы. Поэтому в настоящее время они имеют широкое применение для хранения и передачи информации.

Однако USB-накопители несут собой двойную угрозу, потому что позволяют пользователям тайно скопировать и вынести за территорию предприятия конфиденциальную или охраняемую информацию, а также подвергнуть риску заражения вредоносным ПО информационную систему или отдельный компьютер, причем, как правило, без активных действий пользователя.

Защита от утечек конфиденциальной информации является одной из приоритетных задач для IT-отдела любого банка.

Утечки из банка конфиденциальной информации на USB-устройствах способны не только ослабить его позиции в конкурентной борьбе, но и существенно ухудшить отношение к этому банку со стороны клиентов и государственных структур. В этом плане наиболее опасной оказывается утечка данных о клиентах (как частных, так и корпоративных) и/или о проводимых ими финансовых операциях.

Можно выделить следующий перечень угроз информационной безопасности (утечек) для банковского сектора:

- При уходе сотрудника в другую организацию. Уходящие специалисты с помощью USB-накопителей могут унести с собой разного рода конфиденциальную информацию — например, обсуждаемые бизнес-идеи, применяемые технологии, данные о ключевых клиентах и т.д.;
- Информация по корпоративным клиентам. Обычно с крупными корпоративными клиентами банки работают индивидуально — на особых условиях. Если эти условия становятся известны конкурентам, те могут попросту переманить корпоративного клиента, предложив более выгодные условия сотрудничества;
- Информация о проводимых банковских транзакциях — кто, куда и какие суммы переводит. Практически всегда обнародованный факт такой утечки приводит к фатальному оттоку клиентов и подрыву доверия к банку;
- Информация о разрабатываемых маркетинговых программах, инновациях в этой сфере.
- Утечка информации об инвестиционных планах банка способна привести к срыву важных и потенциально очень доходных проектов.
- Информация о системе безопасности банка.

Закрытие USB портов компьютера не улучшит ситуацию. Гораздо лучший подход заключается в том, чтобы определить порядок работы с внешними электронными носителями в политике информационной безопасности предприятия.

Чтобы избежать утечки конфиденциальной (охраняемой) информации и заражения IT-ресурсов вредоносными программами, которые могут быть принесены на внешнем электронном носителе, компьютеры должны быть защищены соответствующим образом. ПО, предназначенное для защиты, должно регламентировать работу с внешними электронными носителями, а также блокировать на них вредоносный код.

Сегодня в мире достаточно производителей ПО, способного контролировать периферийные устройства. В России это, например, Device Lock — продукт компании Смарт Лайн и Zlock — продукт компании Securit.

Комплексные решения на белорусском рынке

Компания «ВирусБлокАда» добавило в антивирусный комплекс Vba32 модуль, направленный на решение проблемы несанкционированного использования в корпоративной сети периферийных устройств, прежде всего внешних электронных носителей, с помощью которого можно ограничивать доступ пользователей к внешним устройствам (например, к USB-устройствам и внешним накопителям).

Центр управления Vba32 позволяет конфигурировать специализированный драйвер управления внешними электронными носителями, который является частью антивирусного комплекса Vba32. Основная задача управления доступом к съёмным носителям заключается в назначении определенного действия драйвера управления по отношению к конкретному USB-накопителю. Администратор центра управления определяет поведение драйвера управления на конкретной рабочей станции. При этом для каждого компьютера могут быть заданы свои настройки действия над определенным устройством.

Защита USB-накопителей во взаимодействии с антивирусом не дает пользователям тайно скопировать конфиденциальную информацию с ПЭВМ, а также внедрить вредоносное и шпионское ПО на отдельно стоящие ПЭВМ и в информационные системы.

Модуль ведет отчет о всех действиях, выполняемых с файлами на USB-накопителе, что особенно важно в случае сбора статистики об обрабатываемой информации и времени ее обработки, а также при расследовании инцидентов, связанных с утечками информации или вирусными заражениями ПЭВМ.

Модуль позволяет реализовать одну из задач, решаемых в целях защиты от несанкционированного доступа к охраняемой информации — аудит действий пользователя при обработке информации на средствах вычислительной техники.

В настоящее время внедрение модернизированного комплекса Vba32 проводится в Национальном банке Республики Беларусь.

ОДО «ВирусБлокАда»
220088, г. Минск,
ул. Смоленская, 15 — 803б
Тел./факс: (017) 294-84-29
E-mail: info@anti-virus.by

УНП: 101294617