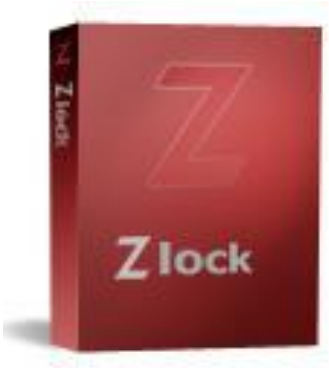
Северный филиал
РГУИТП

Маркова А.В.
гр. И 411

Защита от внутренних угроз. Система Zlock.

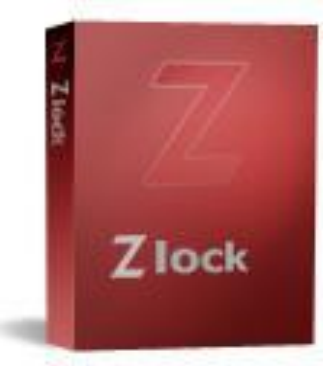


Проблема

Внутренние угрозы безопасности информации становятся все более актуальными.

Это связано с тем, что мобильные накопители нформации, подключаемые через USB порты, например, flash-диски, винчестеры с USB-интерфейсом, уже давно вошли в нашу жизнь как что-то обычное и стандартное.

Система Zlock



Zlock — система защиты информации, предназначенная для управления доступом к портам персонального компьютера, к которым могут подключаться внешние устройства.

Основное назначение системы Zlock – разграничение прав доступа пользователей к внешним устройствам и портам рабочих станций в масштабе предприятия.

Решения

Политика доступа

Разграничение доступа к внешним устройствам в Zlock осуществляется на основе политик доступа. Политика доступа — это логическое понятие, которое связывает описание устройств и прав доступа к ним.

Права доступа могут иметь следующий вид:

- полный доступ;
- доступ только на чтение;
- запрет доступа.

Решения

Каталог устройств

Подключаемые USB-устройства могут идентифицироваться по любым признакам, таким как класс устройства, код производителя, код устройства, серийный номер и т.д.

Это позволяет назначать разные права доступа к устройствам одного класса, например, запретить использование flash-дисков, но при этом разрешить использование принтеров и сканеров.

Решения

Каталог устройств

С помощью каталога можно назначить права доступа для устройства даже в том случае, если оно отсутствует или физически отключено.

Возможен автоматизированный сбор информации об устройствах со всех компьютеров сети и запись ее в каталог устройств, что значительно облегчает последующее управление правами доступа к этим устройствам.

Решения

Сбор событий и их анализ

Система реализует расширенный функционал по ведению и анализу журнала событий.

В журнал записываются все существенные события, в том числе:

- подключение и отключение устройств;
- изменение политик доступа;
- операции с файлами (чтение, запись, удаление и переименование файлов) на контролируемых устройствах.

Решения

Сбор событий и их анализ

В состав Zlock входит средство для анализа журналов, которое обеспечивает формирование запросов любых видов и вывод результатов в формате HTML.

Использование для журнала универсальных форматов хранения данных позволяет воспользоваться любыми сторонними средствами анализа и построения отчетов.

Решения

Теневое копирование

Возможность автоматически выполнять теневое копирование (shadow copy) файлов, которые пользователи записывают на внешние накопители.

Это позволяет контролировать ситуацию даже в том случае, если пользователю разрешена запись на внешние устройства, поскольку администратор безопасности всегда будет точно знать, какую информацию сотрудник записывает на внешние накопители.

Вся информация, записываемая пользователем на внешний носитель, незаметно для него копируется в защищенное хранилище на локальной машине и потом переносится на сервер.

Решения

Теневое копирование

Функция теневого копирования создает точные копии файлов, которые пользователь записывают на устройства, и расширяет возможности аудита, позволяя проводить расследование возможных инцидентов.

Решения

Мониторинг клиентских модулей

Обеспечивает своевременное уведомление администраторов безопасности о подключениях внешних устройств, как запрещенных так и разрешенных, а также о попытках несанкционированной деактивации клиентского модуля и изменения настроек системы.

Это дает возможность службе безопасности оперативно реагировать на несанкционированные действия пользователей и принимать соответствующие меры.

Результаты

Внедрение систем, подобных Zlock, позволит существенно затруднить деятельность инсайдеров и свести к минимуму риск утечки информации с использованием мобильных устройств.

Спасибо за внимание!!!